



Gestionnaire
du Réseau de Transport d'Electricité

Access to RTE's IT system with digital certificates under Microsoft Windows Vista

PKI User Manual

Version 2, 4/11/2008

This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without authorisation in writing from RTE.

CONTENTS

A. Foreword	6
1. Introduction	7
1.1 Document subject	7
1.2 Context	7
1.3 A warning concerning security procedures	8
1.4 The stakeholders	8
1.4.1 <i>The customer</i>	8
1.4.2 <i>The Registration Authority (RA)</i>	9
1.4.3 <i>The Certification Authority (CA)</i>	9
1.5 The certificate management process	9
1.5.1 <i>Issuance of a certificate</i>	9
1.5.2 <i>Renewal of a certificate</i>	9
1.5.3 <i>Revocation of a certificate</i>	10
B. The certificate management procedures	11
2. Request for a digital certificate	12
2.1 Preliminary measures	12
2.2 Overall schematic	12
3. Renewal of certificates	13
4. Revocation of certificates	14
4.1 The revocation scenario	14
4.2 The revocation request	14
5. Incident handling and support	15
5.1 Error codes returned by email	15
5.2 Support	16
C. Workstation configuration	17
6. Installation and configuration of the workstation	18
6.1 Network configuration	18
6.1.1 <i>Overall configuration</i>	18
6.1.2 <i>Particularities of VPN access</i>	18
6.2 Software configuration	19
D. Web browsers	20
7. Internet Explorer	21
7.1 Preliminary configuration	21
7.2 Adding trusted sites	23



7.3	Installation of the RTE CA root certificate	25
7.3.1	<i>Download and installation</i>	25
7.3.2	<i>Contents of the RTE CA certificate</i>	28
7.4	Retrieval of your personal certificate	29
7.4.1	<i>Generation of the key pair</i>	31
7.4.2	<i>Contents and verification of your digital certificate</i>	33
7.5	Use of your certificate	35
7.5.1	<i>Authentication and encryption</i>	35
7.5.2	<i>Example of accessing the "RTE Customer Services Portal"</i>	36
7.6	Supplementary operations	37
7.6.1	<i>Export of your personal certificate</i>	37
7.6.2	<i>Import of your personal certificate</i>	40
7.6.3	<i>Deletion of your personal certificate</i>	43
7.7	Connection to the SSL VPN	45
7.7.1	<i>Foreword</i>	45
7.7.2	<i>Prerequisites</i>	45
7.7.3	<i>First connection</i>	45
7.7.4	<i>Use of the SSL VPN</i>	47
8.	Mozilla Firefox	49
8.1	Preliminary configuration	49
8.2	Installation of the RTE CA root certificate	49
8.2.1	<i>Download and installation</i>	49
8.2.2	<i>Verification of the root certificate fingerprint</i>	50
8.3	Retrieval of your personal certificate	54
8.3.1	<i>Generation of the key pair</i>	56
8.3.2	<i>Installation of the certificate</i>	56
8.3.3	<i>Viewing and verification of your digital certificate</i>	57
8.4	Use of your certificate	59
8.4.1	<i>Authentication and encryption</i>	59
8.4.2	<i>Example of accessing the "RTE Customer Services Portal"</i>	59
8.5	Supplementary operations	61
8.5.1	<i>Export of your personal certificate</i>	61
8.5.2	<i>Deletion of your personal certificate</i>	67
8.6	Connection to the SSL VPN	69
8.6.1	<i>Foreword</i>	69
8.6.2	<i>Prerequisites</i>	69
8.6.3	<i>First connection</i>	69
8.6.4	<i>Use of the SSL VPN</i>	72
E.	Email clients	75
9.	Use of email clients	76
9.1	Certificates and email software	76

9.2	When to use the certificate	76
10.	Windows Mail	78
10.1	Preliminary configuration	78
10.2	Use of the certificate	80
10.2.1	<i>When to use the certificate</i>	80
10.2.2	<i>Application certificates</i>	81
10.2.3	<i>Message encryption and signing</i>	82
11.	Outlook 2003	83
11.1	Preliminary configuration	83
11.2	Use of the certificate	85
11.2.1	<i>When to use the certificate</i>	85
11.2.2	<i>Application certificates</i>	85
11.2.3	<i>Message encryption and signing</i>	86
12.	Outlook 2007	89
12.1	Preliminary configuration	89
12.2	Use of the certificate	91
12.2.1	<i>When to use the certificate</i>	91
12.2.2	<i>Application certificates</i>	91
12.2.3	<i>Message encryption and signing</i>	93
13.	Mozilla Thunderbird	95
13.1	Preliminary configuration	95
13.2	Use of the certificate	96
13.2.1	<i>When to use the certificate</i>	96
13.2.2	<i>Application certificates</i>	96
13.2.3	<i>Message encryption and signing</i>	98
13.3	Importing the certificate	99
13.4	Deletion of the certificate	104
14.	Lotus Notes	106
14.1	Importing the certificate	106
14.2	Viewing the certificate	114
14.3	Reception of a signed and encrypted message	115
14.4	Signature and encryption of messages sent	117
F.	Appendices	120
15.	PKI Secured environments	121
15.1	Concepts and objects generated by a PKI	121
15.1.1	<i>What is a secured process?</i>	121
15.1.2	<i>The role of the key pair</i>	122
15.1.3	<i>The certificates</i>	124
15.2	Documentation	125
16.	Glossary	127



Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



A. FOREWORD

1. Introduction

1.1 Document subject

This document is intended for the end user who wishes to access the RTE's IT system with digital certificates.

This document allows certificate holders to:

- understand the context and the principles of a secured environment, as well as the general operation of a public key infrastructure (PKI, or IGC in French).
- know how to install and use their digital certificates in the following environments:
 - o Windows Vista,
 - o Browsers: Mozilla Firefox and Internet Explorer 7 for secure access using the HTTPS protocol and through an SSL VPN,
 - o Email clients: Mozilla Thunderbird 2, Outlook 2003/2007, Windows Mail, Lotus Notes 7 (at least 7.0.2) for secure communications in the S/MIME format.

NOTE

Throughout this document, the pronoun "you" is used to reference the certificate holder. References to he/him/his/himself are for brevity and are also implied to refer to she/her/hers/herself wherever they occur.

1.2 Context

In the context of the February 10th 2000 legislation (2000-108) and the implementing decree 2001-630 of July 16th 2001, the administrator of a public transport network has an obligation to protect the confidentiality of all information of economic, commercial, industrial, financial or technical natures whose communication might adversely impact the rules of free and fair competition and non-discrimination as defined by the law.

1.3 A warning concerning security procedures

Each holder of a digital certificate uses a cryptographic module of their web browser to maintain their own securely-generated private key on the hard drive of their workstation. Therefore, every digital certificate holder must take the necessary precautions to prevent:

- the breach of their private key;
- the loss of their private key;
- the disclosure of their private key;
- the modification of their certificate;
- and any abusive use of their certificate.

Every certificate holder has, and recognises having, complete responsibility for the protection of their private key(s). The private keys and their associated certificates are stored on the hard disk, hence their being known as "digital" certificates; these private digital keys can be protected by a password only known by the certificate holder.

The Certification Authority (CA) of "RTE France" declines all responsibility relating to litigation arising or associated with inappropriate use of these private keys.

Please refer to:

- chapter 2 of the ***Certification Policy of the RTE France CA***, which is found in the package that has been supplied to the company manager:
<PACKAGE>\RTE Installation\fr\Politique de Certification RTE.pdf
- the ***IT System access regulations***.
<PACKAGE>\Sécurité - Charte d'utilisation des certificats logiciels.pdf

1.4 The stakeholders

Certificate lifecycle management revolves around three entities:

- the customer (i.e. your company),
- the Registration Authority (RA),
- the Certification Authority (CA).

NOTE

To make things easier to understand, an analogy can be made with the allocation of official identity documents: a citizen requesting an identity document corresponds to the customer entity, the municipality acts as the registration authority, and the central Internal Affairs department as the certification authority.

1.4.1 The customer

The customer makes certificate requests on behalf of its certificate holders. The customer can similarly issue requests for revocation of those certificates.

1.4.2 The Registration Authority (RA)

The Registration Authority (the RTE customer relations officer for the Operator's team) receives a certificate request and verifies the identity of the certificate holders who will be using the certificates.

1.4.3 The Certification Authority (CA)

The (RTE) Certification Authority is responsible for and vouches for the certificates signed in its name and for the smooth operation of the PKI. It defines its own policies for the administration and usage of its certificates.

The RTE certification authority is defined as:

CN = RTE Autorité de Certification, O = RESEAU DE TRANSPORT D ELECTRICITE

1.5 The certificate management process

The principle processes implemented to manage the combined collection of digital certificates delivered to certificate holders are as follows:

- the issuance of a certificate (issuance of one or more certificates),
- the renewal of a certificate (replacing someone's certificate with a new one for a new validity period and for a new key pair,
- the revocation of a certificate.

The RTE's certification policy is available on the RTE corporate internet site.

1.5.1 Issuance of a certificate

Certificates are issued in compliance with the RTE Certification Policies upon the initiative of the company representative for contractual relationships with RTE.

The requests are issued by the customer through its RTE customer relations officer, who forwards them to the appropriate groups to register the certificate holder. Then the certificate holder himself registers on the site assigned for digital certificates. After that, the browser generates a key pair on the certificate holder's workstation and downloads the associated certificate.

1.5.2 Renewal of a certificate

Forty days before the expiry of a certificate, an electronic message is sent to the certificate holder to inform him of the renewal of his digital certificate.

If modifications need to be made relating to the certificate holder's details, then the company's representative contacts the RTE customer relations officer to tell him what those changes are.

Otherwise an email is sent to the certificate holder with the information necessary for the retrieval of his new certificate.



1.5.3 Revocation of a certificate

For scenarios involving a change of the certificate holder, loss or a compromised certificate, the company manager directly contacts the RTE Hotline to request the revocation of that certificate. The customer will be notified of the revocation of that certificate. The revocation request may originate from RTE itself in the event of fraud.



B. THE CERTIFICATE MANAGEMENT PROCEDURES

2. Request for a digital certificate

2.1 Preliminary measures

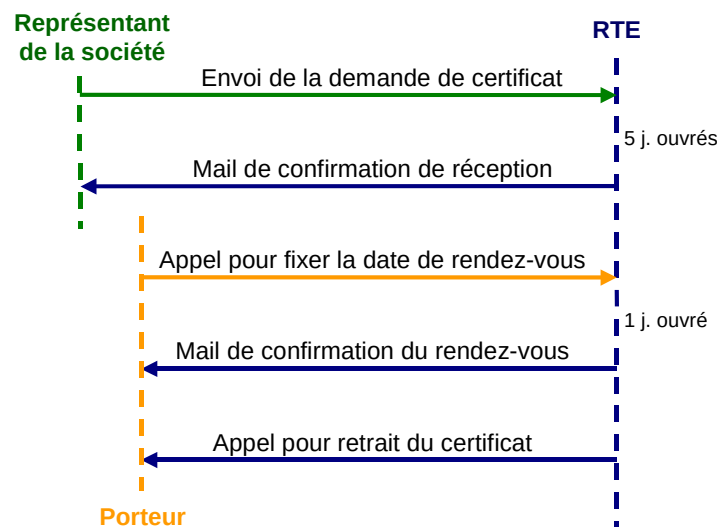
The following steps must have been completed in advance:

- **The company representative has made an access request:**
the company representative must have filled out and signed the "RTE IT System and Applications Access Request Forms"; and must have sent them to the RTE customer relations officer;
- **We have registered your request:**
upon reception of those forms, we will have created your application access account(s).

2.2 Overall schematic

Once the certificate request has been registered and validated by our services (within 5 working days), a message will be sent to the company manager to acknowledge receipt of the forms and asking him to call us to fix a phone meeting with the certificate holder for the day of the certificate installation.

Then, a message will be sent to the certificate holder after this call, reminding him of the scheduled meeting and giving him the address of the download web site and the retrieval code which will allow him to download his certificate from his own workstation.



The certificate holder must then connect to the digital certificate administration web site from his workstation to fill out and validate the registration form online. At that moment, a key pair will be generated on his workstation and his certificate will be downloaded.



3. Renewal of certificates

Certificates have a validity of two years so that a high level of security can be delivered with them.

Forty days before the expiry of a certificate, an electronic message is sent to the certificate holder to inform him of the renewal of his digital certificate.

If modifications need to be made relating to the certificate holder's details, then the company's representative contacts the RTE customer relations officer to tell him what those changes are.

Otherwise an email is sent to the certificate holder with the information necessary for the retrieval of his new certificate.

4. Revocation of certificates

4.1 The revocation scenario

The company manager must issue a revocation request whenever one of the following circumstances arises:

- change of the certificate holder,
- loss, theft, compromise, or suspicion of possible, probable or certain compromise of the private key associated with the holder's certificate,
- death or discontinuation of employment of the certificate holder,
- loss of the activation data, or defective or lost removable media.

4.2 The revocation request

To revoke a certificate, the company manager should call the RTE Hotline and supply the PKI User Credentials, such as were provided in the forms for requesting access to the RTE IT systems.

5. Incident handling and support

In the event of a problem, the company manager will contact the RTE Hotline (see §5.2), who will diagnose the problem and forward it to the corresponding technical expert concerned. The Hotline will later forward the solution to the company manager and assist him where necessary to apply the procedures indicated to regain access to the RTE IT systems.

5.1 Error codes returned by email

During an exchange of electronic messages between the user and an application, even if the certificate was generated and installed according to the procedures described in the rest of this document, it is possible that a functionality error may occur. In such events, the component (e.g. a server, a router) in question returns an error code by email.

The subjects of the error messages returned by the **cryptographic router** are of the form:

<ERR:nnn!!<FR Description>!!<EN Description>> <Subject-of-the-original-message>

nnn	Description	Possible cause
001	The email sent by the customer has neither been signed nor encrypted	You have not checked the signing and encrypting boxes in your email software when you sent the email
002	The email sent by the customer has only been encrypted	You did not check the signing box in your email software
003	The email sent by the customer has only been signed	You did not check the encrypting box in your email software
004	The email sent by the customer has only been signed and the signature used is incorrect	You did not check the encrypting box in your email software and the certificate that you used to sign the message is invalid or unknown
005	The email sent by the customer has been signed and encrypted, but the signature used is incorrect	The signature certificate that you used is invalid or unknown
006	The email sent by the customer could not be decrypted by RTE	That certificate that you used to encrypt the email is invalid
007	The email sent by RTE did not reach the customer because of a security problem	This is an internal RTE problem

<FR-Description>

Description of the error in French.

<EN-Description>

Description of the error in English.



**<Subject-of-the-original-
message>**

The subject header of the original message that caused the error in question.

5.2 Support

For any information or assistance, the customer can contact the **RTE Hotline** at:

00 800 80 50 50 50
(universal green number)



C. WORKSTATION CONFIGURATION

6. Installation and configuration of the workstation

All operations in this chapter are to be performed just once by computer staff with **Administrative privileges over your workstation when you receive your RTE applications access kit.**

In addition, note that **only a few chapters of this manual** concern you directly: those being the chapters relating to the software that you use.

6.1 Network configuration

6.1.1 Overall configuration

Electronic messages (emails) passing between RTE and the user will be transported over the Internet (SMTP protocol, S/MIME format).

Access with a web browser employs – quite transparently to the user – a digital certificate access authentication system for the RTE portal and encryption of data communicated over the Internet (HTTPS protocol).

IMPORTANT NOTE

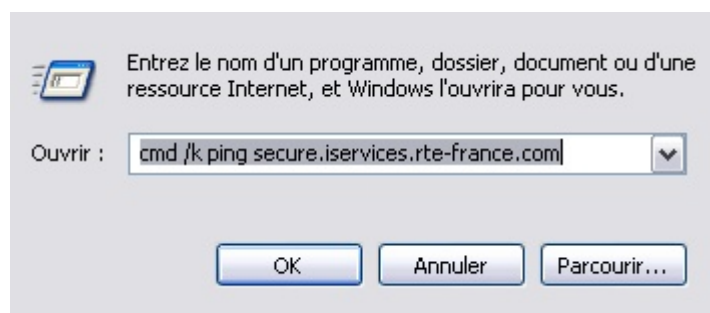
The messaging and antivirus routers, firewalls and content analysers must be configured to not alter or refuse encrypted and signed messages in S/MIME format (application/x-pkcs7-mime, .p7s, .p7m), nor to block HTTP data traffic (port 443).

The network administrator can be consulted to perform these operations

6.1.2 Particularities of VPN access

Access to the SSL VPN requires that your workstation is able to resolve and access the address: **secure.iservices.rte-france.com**. To verify if this is the case, open your Start menu and click on Run. In the window that appears, enter this command:

cmd /k ping secure.iservices.rte-france.com



Click on the **"OK"** button.

A window will appear containing some information:

- If the first line starts with **"Sending a ping request to secure.iservices.rte-france.com"**, then the address

secure.iservices.rte-france.com has been resolved. Your workstation is correctly configured.

- If the first line starts with "**The ping request could not locate the server secure.iservices.rte-france.com**", then the address **secure.iservices.rte-france.com** has not been resolved. Please contact your IT support desk so that they can make the necessary changes to enable the ping/address resolution.

6.2 Software configuration

The software configuration required for your workstation is as follows:

Operating systems:

- Windows Vista (all versions).

Web Browsers , *either of:*

- Internet Explorer 7,
- Mozilla Firefox 2.x (For accessing the SSL VPN, the maximum version is 2.0.0.14).

Email clients , *any one of:*

- Windows Mail,
- Outlook 2003 and 2007,
- Mozilla Thunderbird 2.x,
- Lotus Notes 7 starting from version (7.0.2).



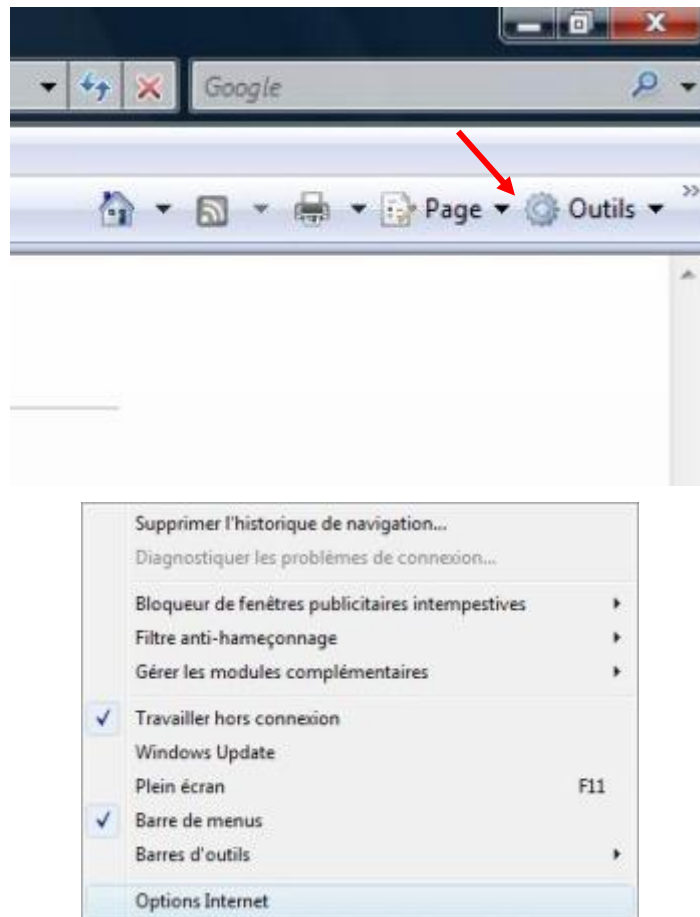
D. WEB BROWSERS

7. Internet Explorer

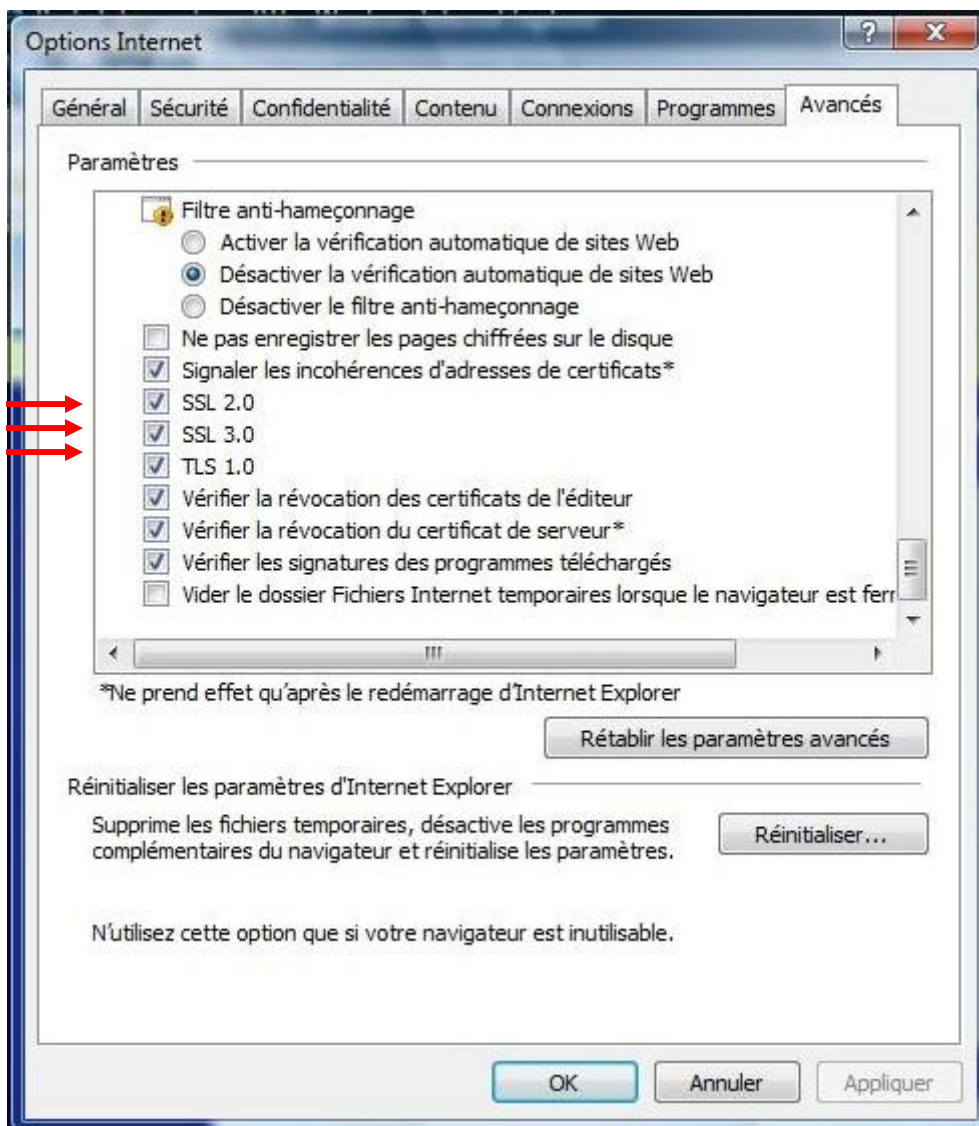


7.1 Preliminary configuration

In the browser, select the "**Tools > Internet options...**" menu options:



Select the "**Advanced**" tab:

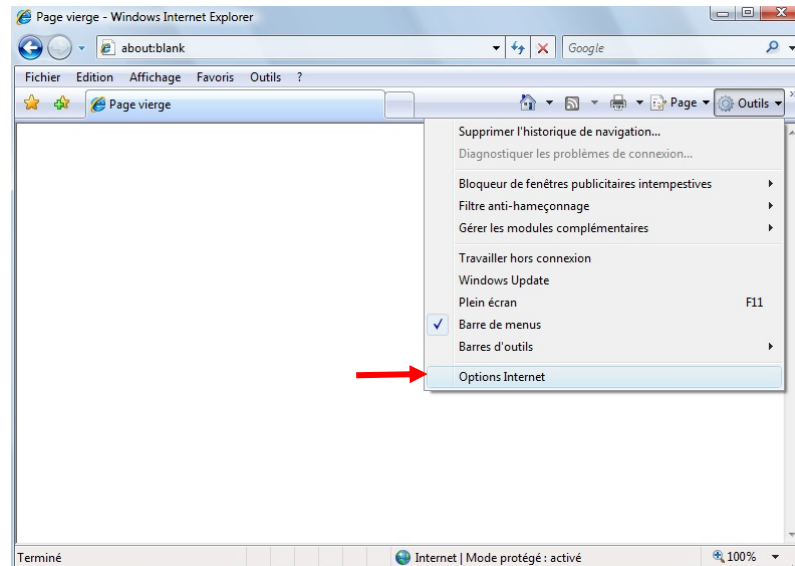


In the section labelled "**Security**", makes sure that checkboxes for SSL 2.0, SSL 3.0 and TLS 1.0 have been checked, as shown above.

7.2 Adding trusted sites

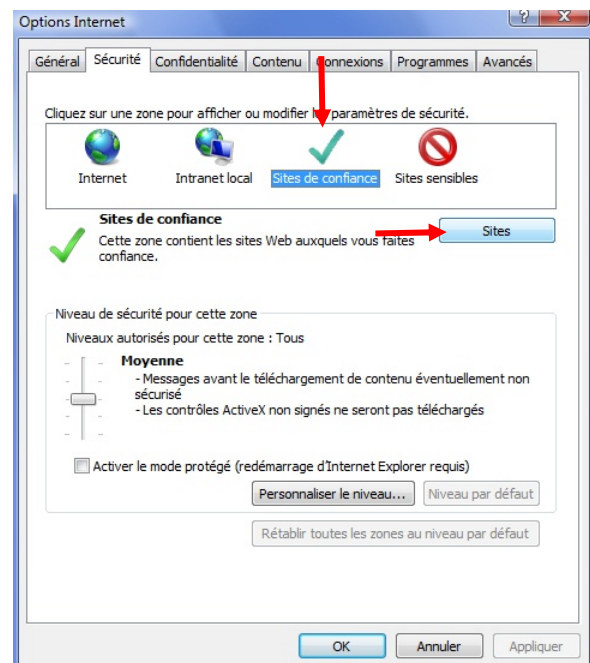
In order to be able to authenticate yourself to Internet sites with your digital certificate, it is absolutely necessary to add these sites to the list of trusted sites.

To do so, open Internet Explorer and click on the "Tools > Internet options" menu option.



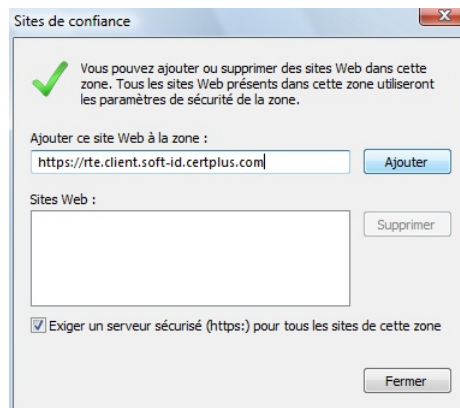
In the window that opens, click on the "Security" tab.

Select the "Trusted sites" icon, then click on the "Sites" button



Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual

The following window opens.

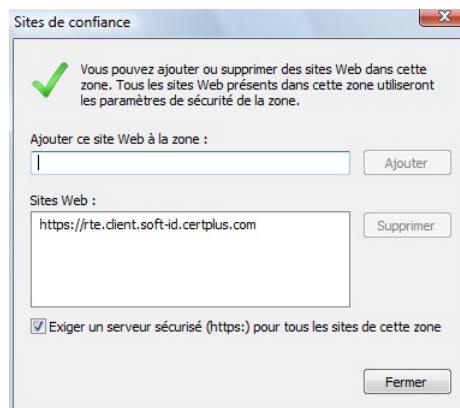


In the field "Add this web site to the zone", enter the following URL:

<https://rte.client.soft-id.certplus.com>

Click on the "Add" button.

The site will now appear in the "Web Sites" list as shown on the screen below.

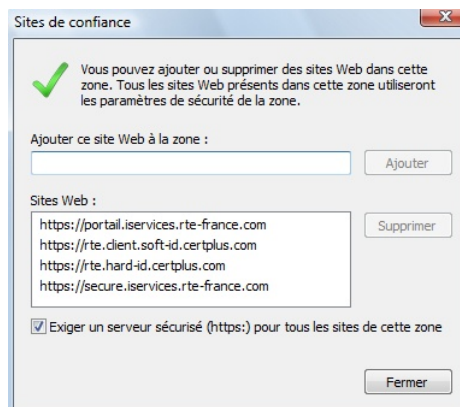


Continue in the same fashion to add the following sites:

<https://portail.iservices.rte-france.com>

<https://secure.iservices.rte-france.com>

The 4 sites should now appear in the "Web Sites" list.



Click on "Close" and then on "OK".

7.3 Installation of the RTE CA root certificate

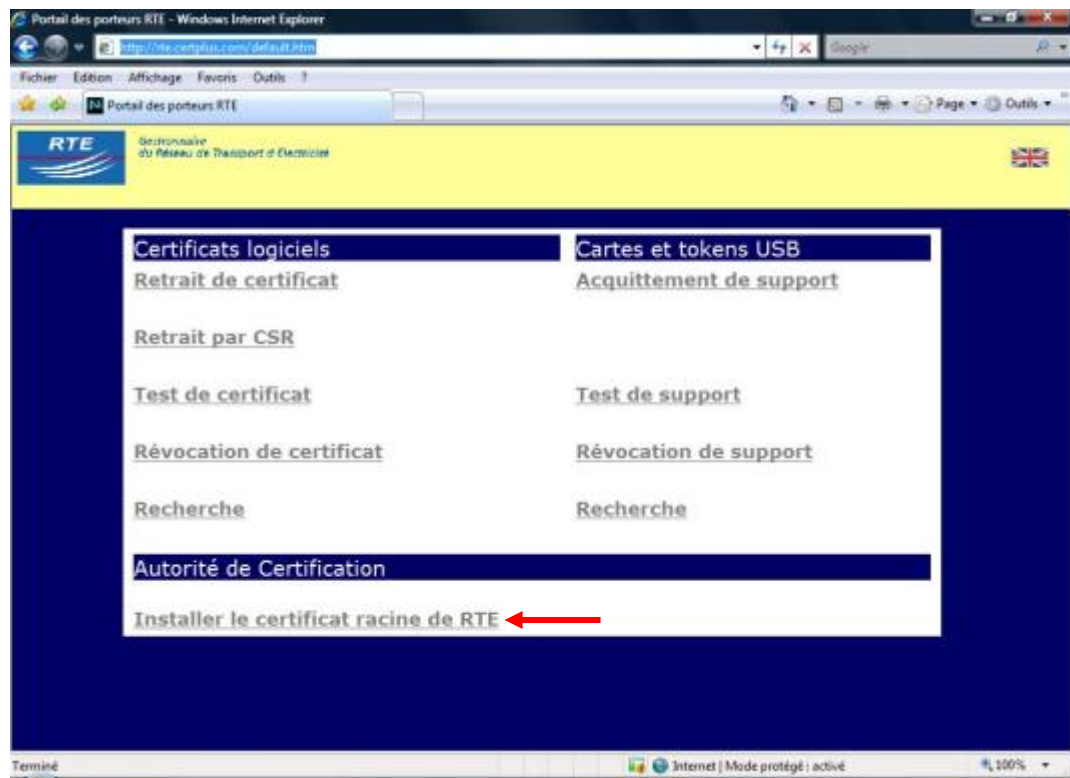
7.3.1 Download and installation

The RTE root certificate must now be installed in your browser so that RTE is known as the trusted Certification Authority.

To do this, please navigate to the RTE customer site at the following address:

<http://rte.certplus.com/default.htm>

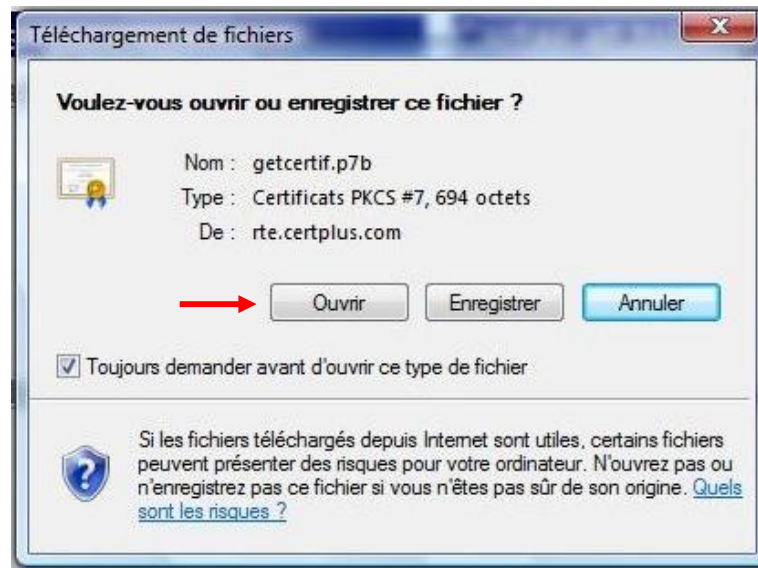
The following page will be displayed.



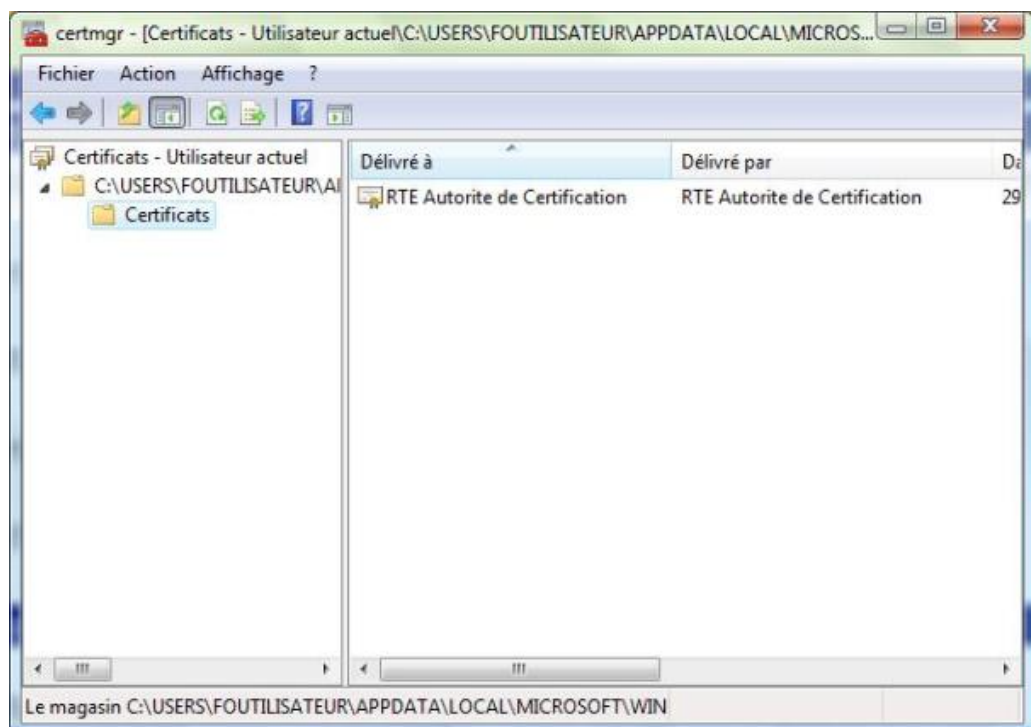
Click on the link "Installer le certificat racine de RTE / Install the RTE root certificate"

The RTE CA root certificate will then be installed in the Windows certificate store, as per the process described below.

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual

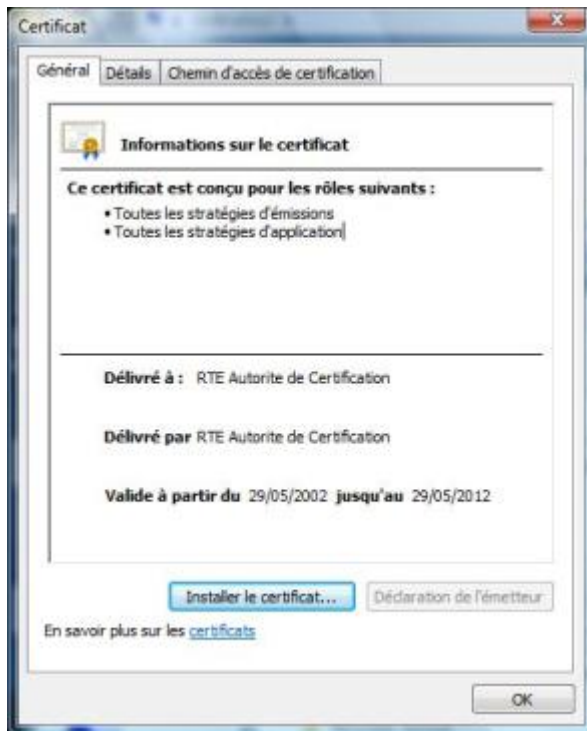


Click on the **"Open"** button.



Double-click on **"RTE Autorite de Certification (RTE Certification Authority)"**.

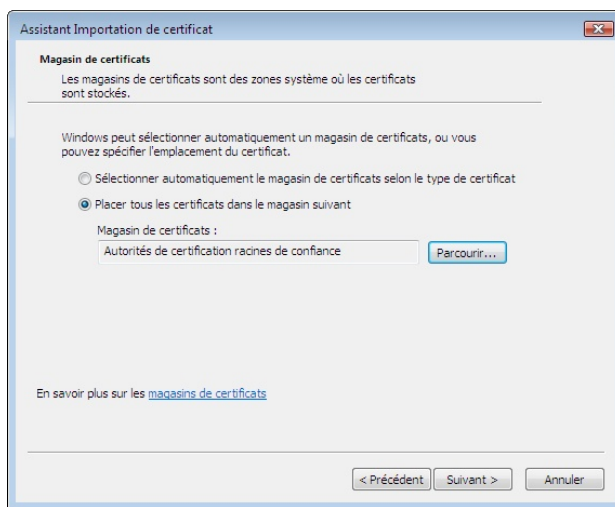
Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



Click on the **"Install the certificate"** button.



Click on **"Next"**.



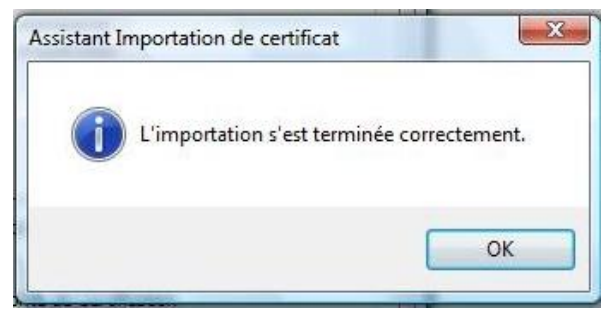
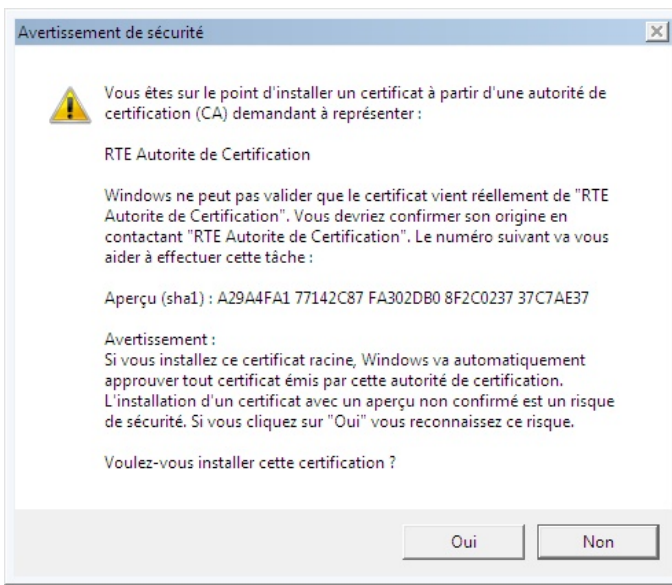
Check the box labelled **"Put all the certificates in the following store"** and click on **"Browse"**.

In the window which opens, select **"Trusted root certification authorities"** and click on **"OK"**.

Click on **"Next"**.



Click on **"Finish"**, and the following window then displays the contents of the root certificate to be imported.



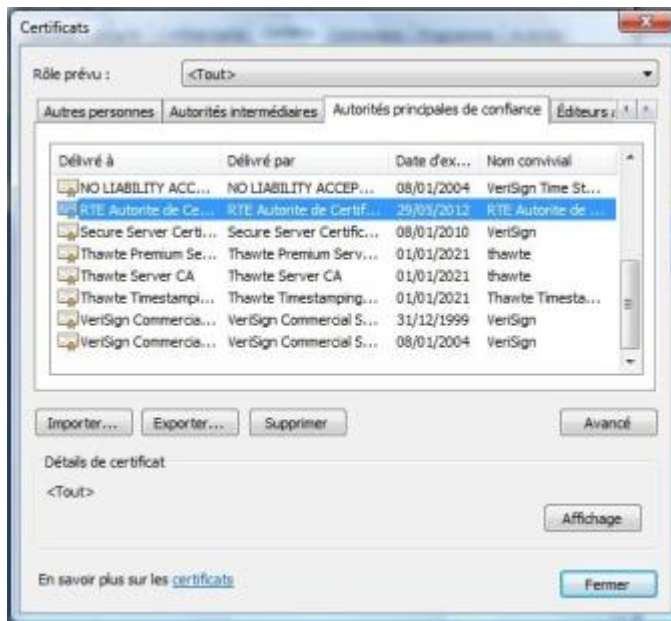
Click on "OK".

Click on "Yes" (verification of the RTE CA certificate will be discussed in the next chapter).

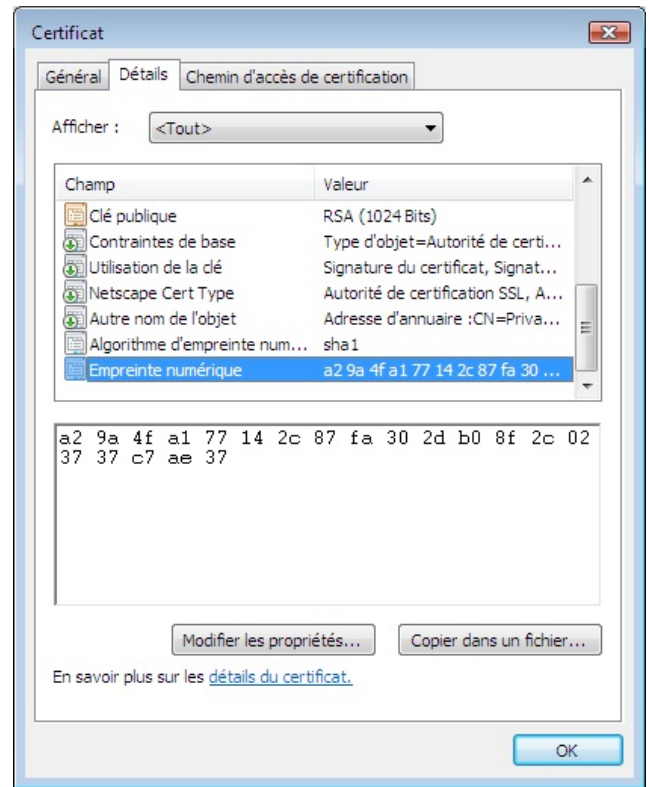
7.3.2 Contents of the RTE CA certificate

The root certificate that you have just downloaded is stored in the certificate store appropriate to the browser used. For example, it can be viewed in Internet Explorer with:

The menu option "**Tools > Internet options...**", "**Contents**" tab, "**Certificates...**" button, "**Trusted root authorities**" tab:



Click on the "**Display**" button, and then on the "**Details**" button.



To make sure that you have downloaded the genuine RTE AC root certificate, carefully check that the "**SHA1**" or "**MD5**" digital fingerprint displayed in the window shown is **identical** to that shown here below.

The **root certificate digital fingerprints** for RTE CA are listed here:

SHA1	A2:9A:4F:A1:77:14:2C:87:FA:30:2D:B0:8F:2C:02:37:37:C7:AE:37
MD5	53:42:6A:2E:A5:10:AB:2A:21:09:EE:88:13:67:A0:31

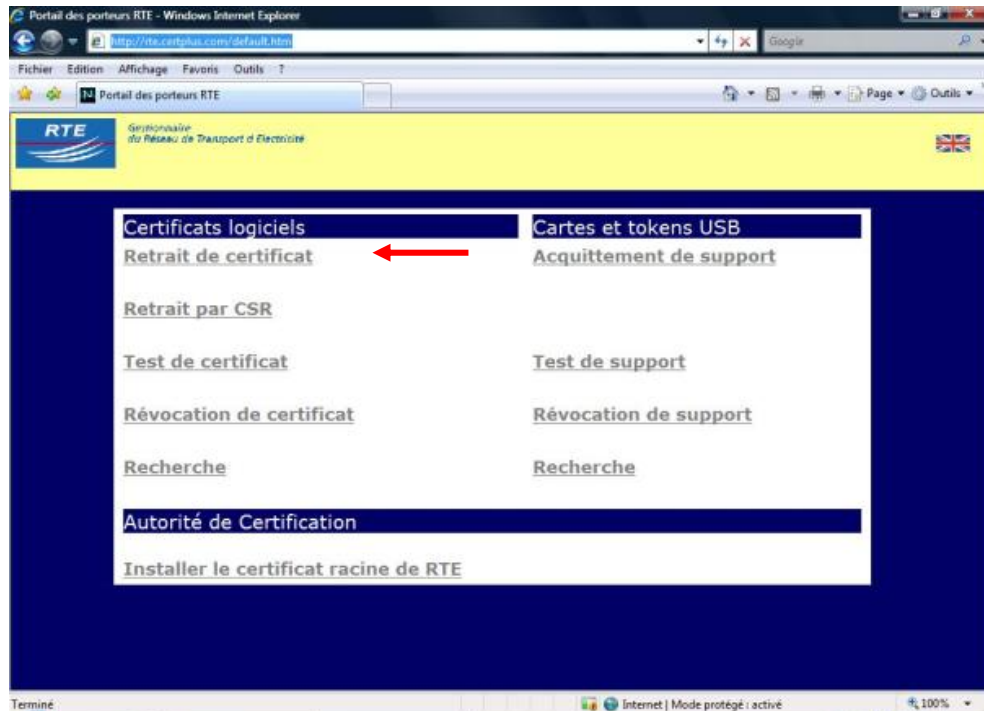
If the hash fingerprint is not identical, delete the certificate and contact our support services.

7.4 Retrieval of your personal certificate

The request for the digital certificate must have been completed as per the procedure laid out in chapter 2

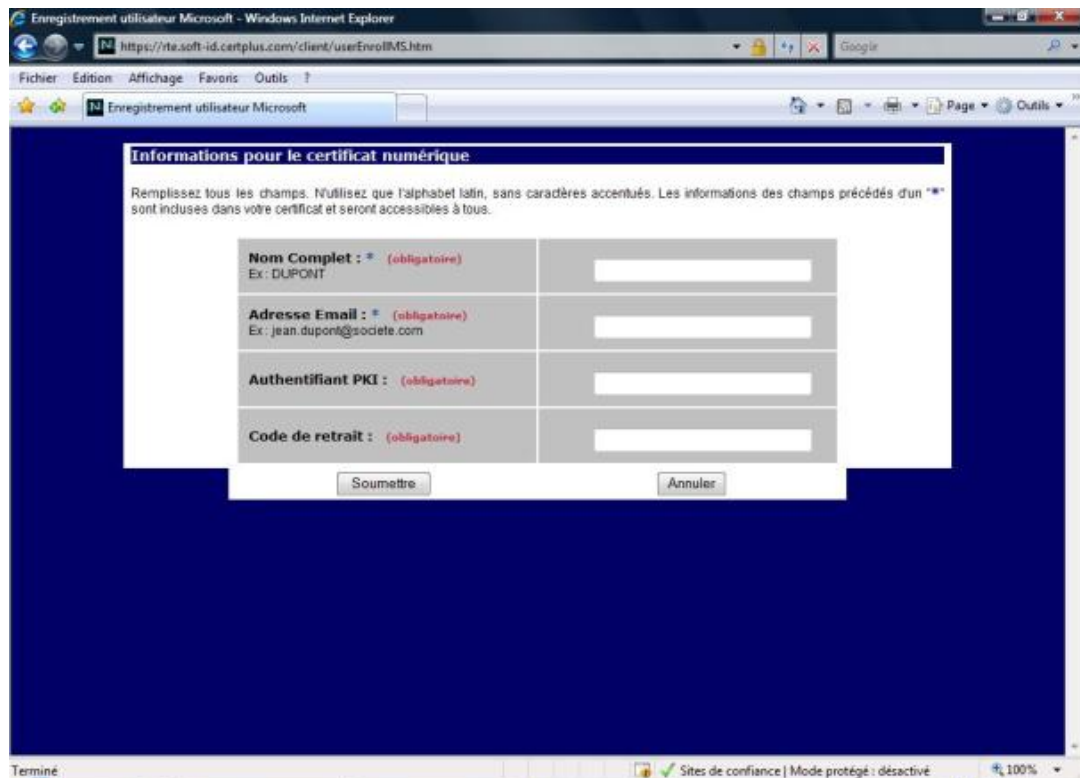
To create your key pair and your certificate, you must then connect, on the RTE meeting day specified, to the web site: <http://rte.certplus.com/default.htm>

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



Click on the "Retrait de certificat / Retrieve the certificate" button.

Fill out the following form:



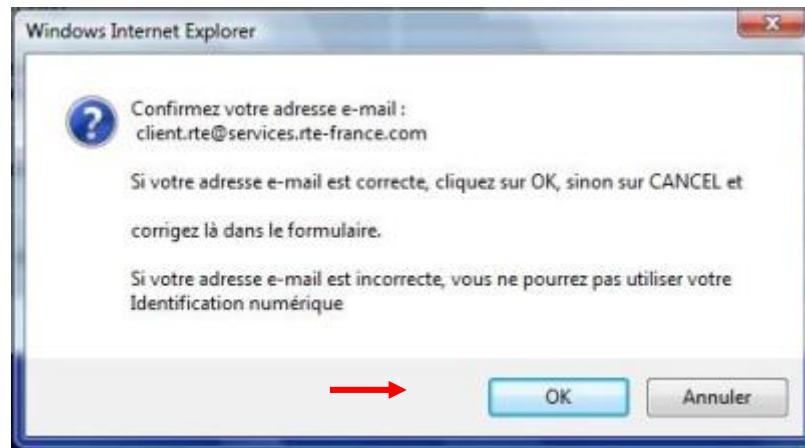
The fields marked with an asterisk must be completed **without diacritic marks** (i.e. accents, cedillas, ...) **or punctuation marks**; as they would also appear in the certificate that will be generated.

The **retrieval code** is the code supplied in the 2nd email that you received from us which allows you to authenticate yourself. To make things easier, you can do simple copy-paste commands to enter the data.

You must likewise enter your **Authentifiant Utilisateur PKI (PKI User Credentials)**, just as they were supplied in the RTE IT system access technical specifications; they will serve to authenticate you with the RTE Hotline any time that you contact them.

Lastly, click on "**Submit**" to send your request for the digital certificate.

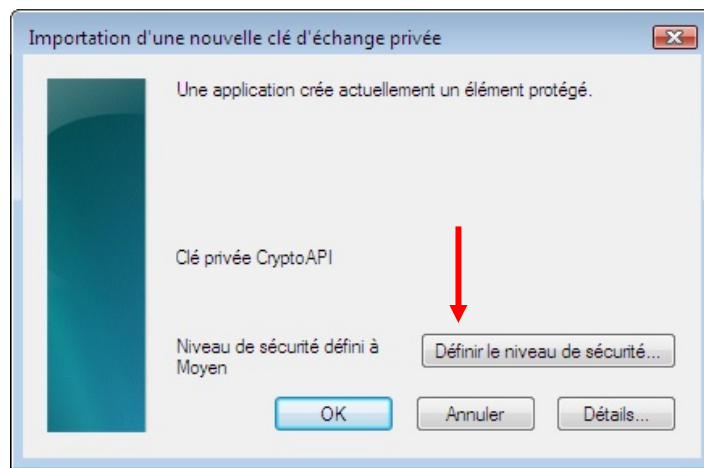
A dialogue box will ask you to confirm your email address:



Click on the "**OK**" button, or "Cancel" to return to the form data entry screen.

7.4.1 Generation of the key pair

The dialogue box shown below will then be displayed, indicating that an RSA key pair has been created by Internet Explorer on your workstation:

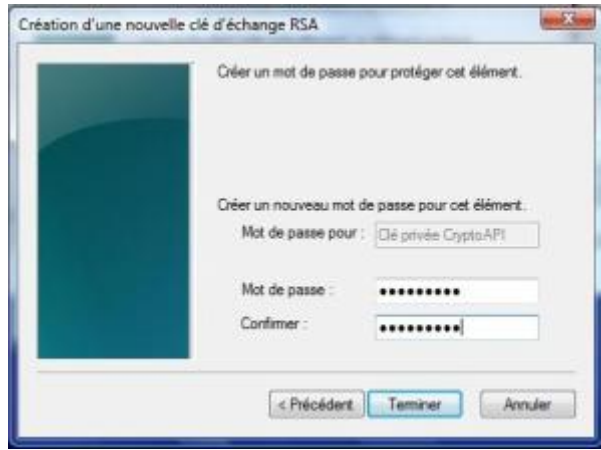
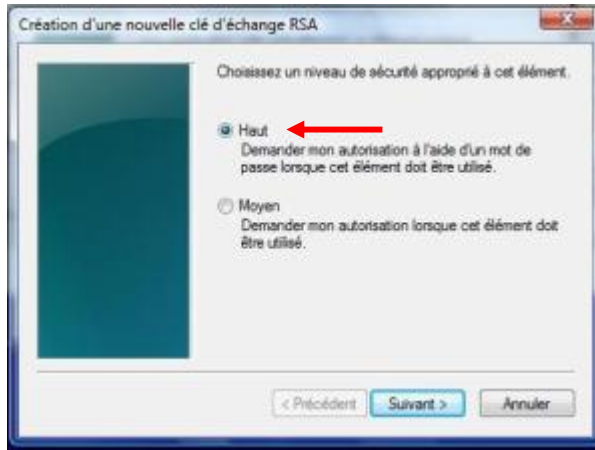


Click on the "**Define the security level**" button.

The key pair that will be generated is, by default, at a "**medium security**" level, which means that each later use of this key pair will cause the display of a simple acknowledgement message: the user is thereby warned of this usage but no password is requested.

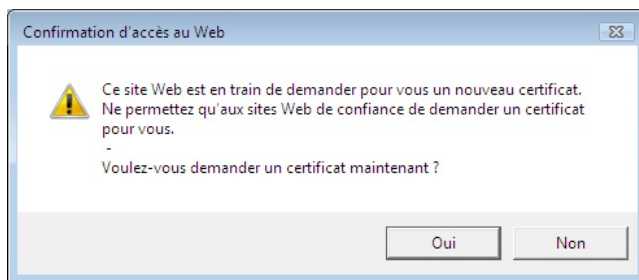
For protected use of your key pair, which we recommend, you should rather choose "**high security**", which will mean that a password, that you will choose

here, will be asked of you for every later use of your key pair. The screens below describe the procedure to set this security level.

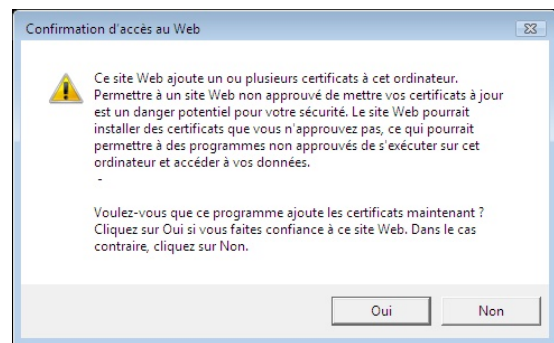


Select the **"High"** option, then click on **"Next"**. Enter a password, then click on the **"Finish"** button.

Click on **"OK"**.



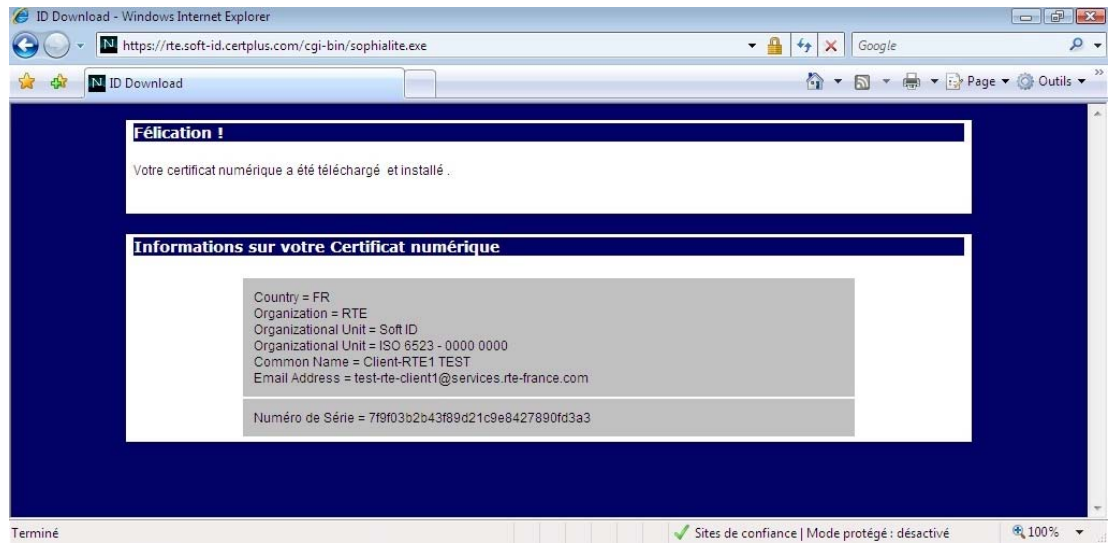
Click on the **"Yes"** button.



Click on the **"Yes"** button.

Installation of the certificate

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



Next, the certificate is automatically downloaded and installed in the Internet Explorer certificate store. The page opposite is displayed to indicate the end of this process.

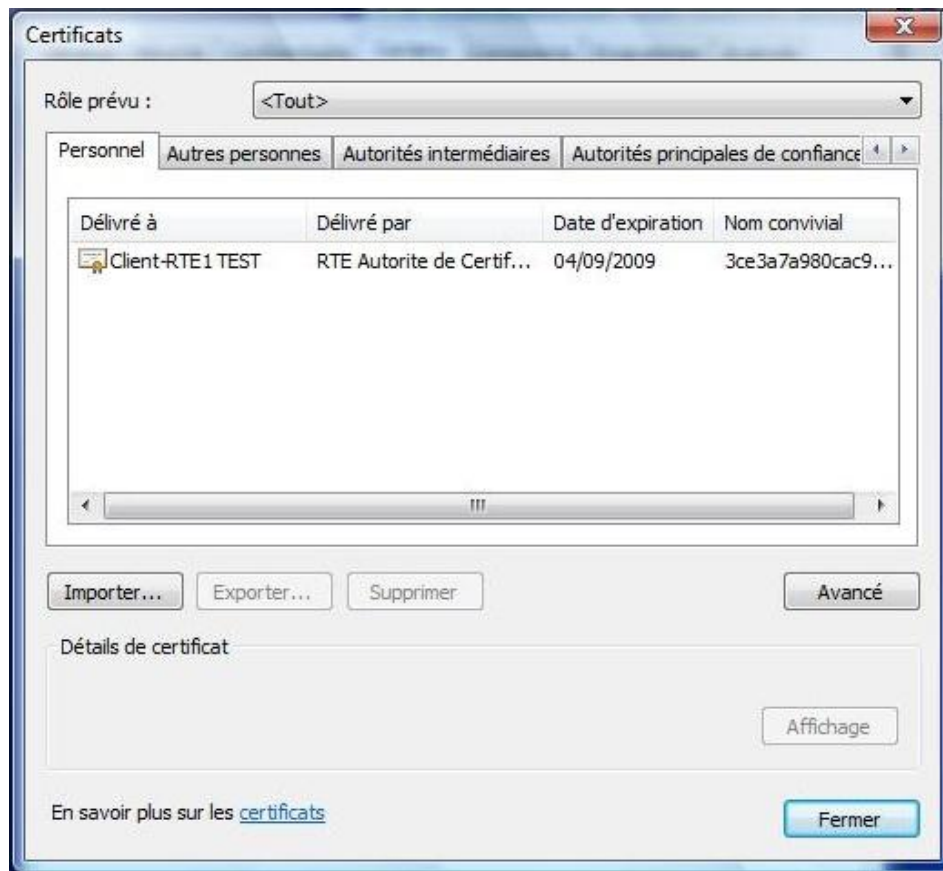
IMPORTANT

Once downloaded, your certificate with its key pair and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to the certificate export procedure §7.6.1.

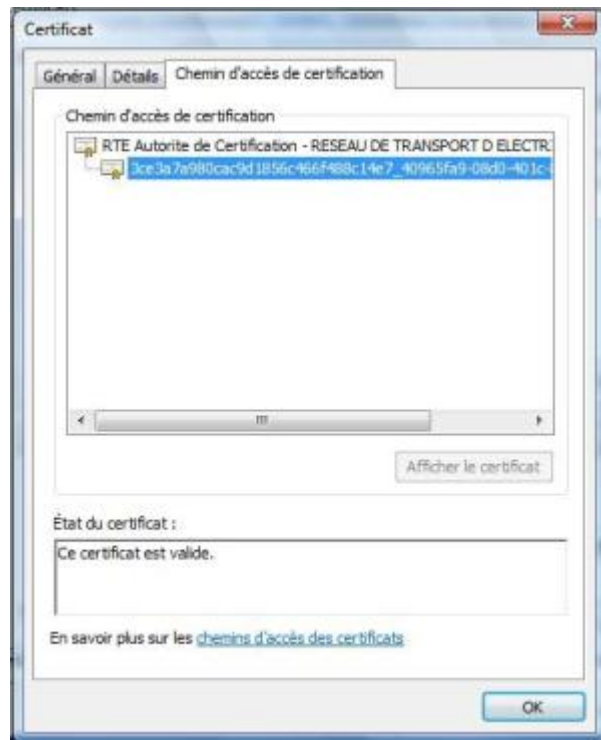
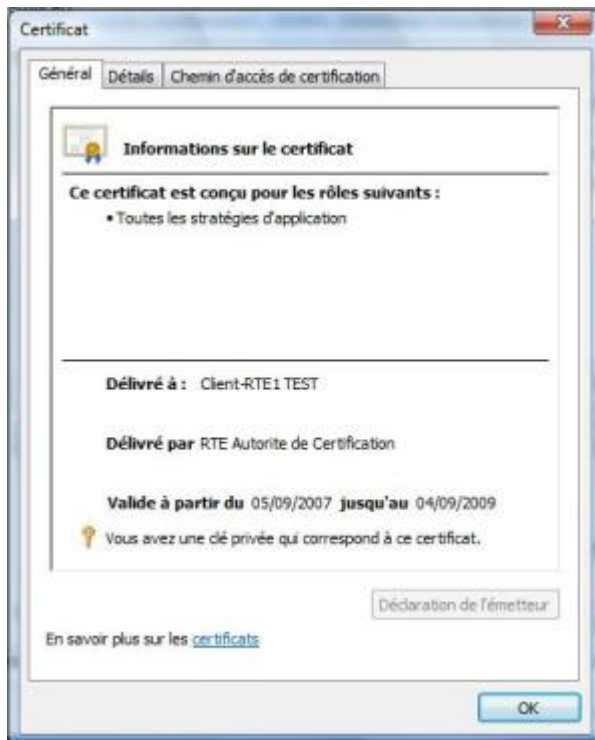
7.4.2 Contents and verification of your digital certificate

Regardless of the browser used, the contents of the downloaded certificate will obviously be the same, only the presentation of the information on the screen will vary. For downloads with Internet Explorer, open the certificate store with the following menu choices:

"Tools > Internet options...", "Contents" tab, "Certificates..." button:

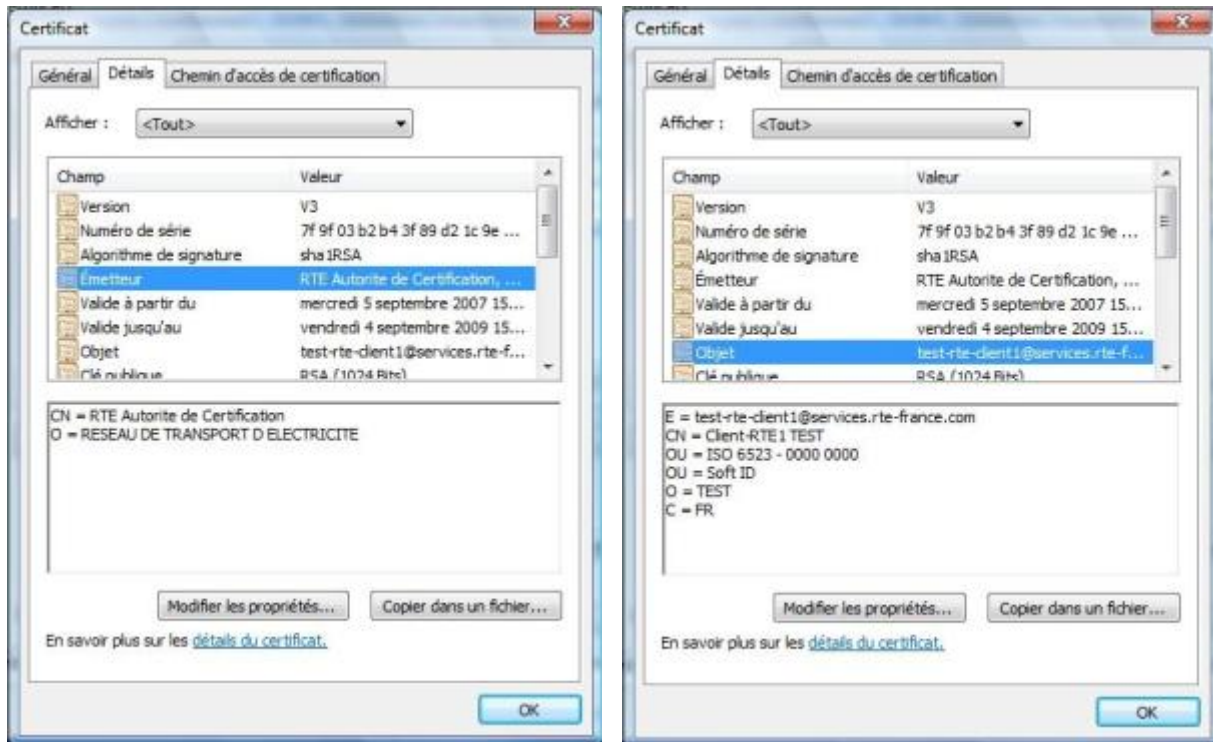


Select your certificate, then click on "Display".



It is valid for 2 years from the download. This tab allows you to verify your certificate date.

The "valid" status of your certificate, as well as the complete display of the certificate access path (2 levels), shows that your certificate has been correctly installed along with the root certificate, and therefore all the correct usage conditions for your certificate have been satisfied.



7.5 Use of your certificate

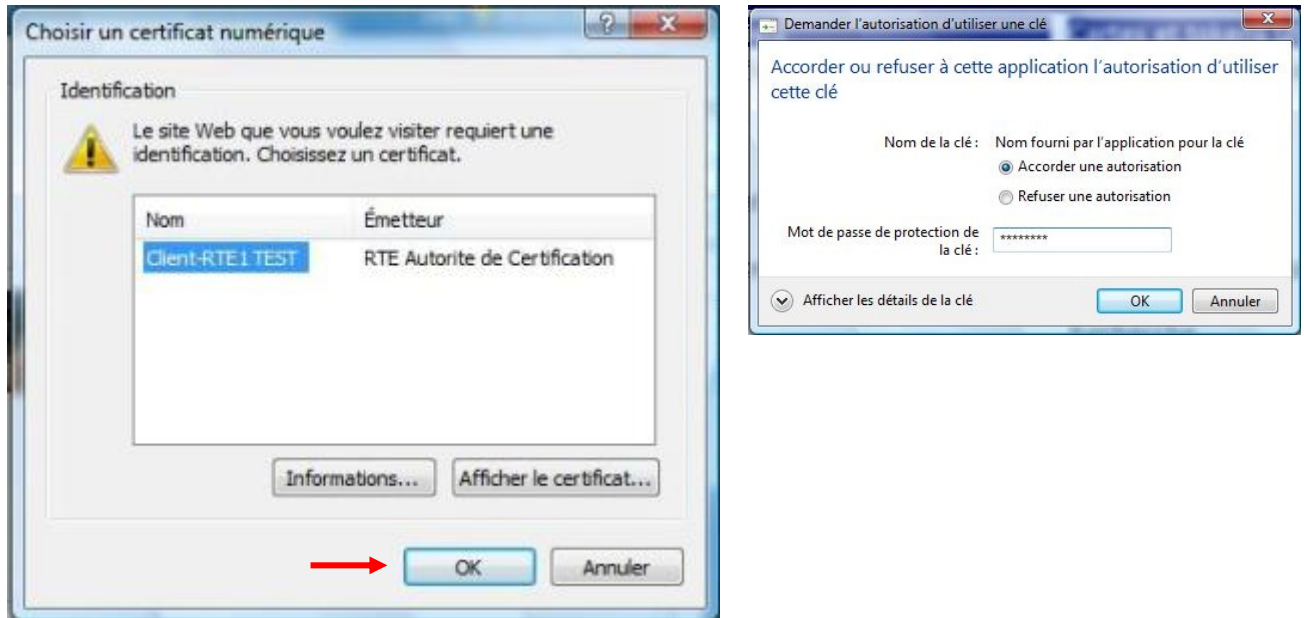
7.5.1 Authentication and encryption

Steps to follow:

- Start Internet Explorer;
- Enter the URL for the RTE application or for the "RTE Customer Services Portal" (this URL starts with "https://");
- During authentication, the browser will ask you to choose the certificate before attempting to authenticate you, and then prompt for the certificate store security password;
- If several certificates are offered to you, you should choose the one that was supplied to you for the application which you are currently attempting to access (use the "Display the certificate" button to look at their contents);
- Now all the data that you send and receive will be encrypted.

7.5.2 Example of accessing the "RTE Customer Services Portal"

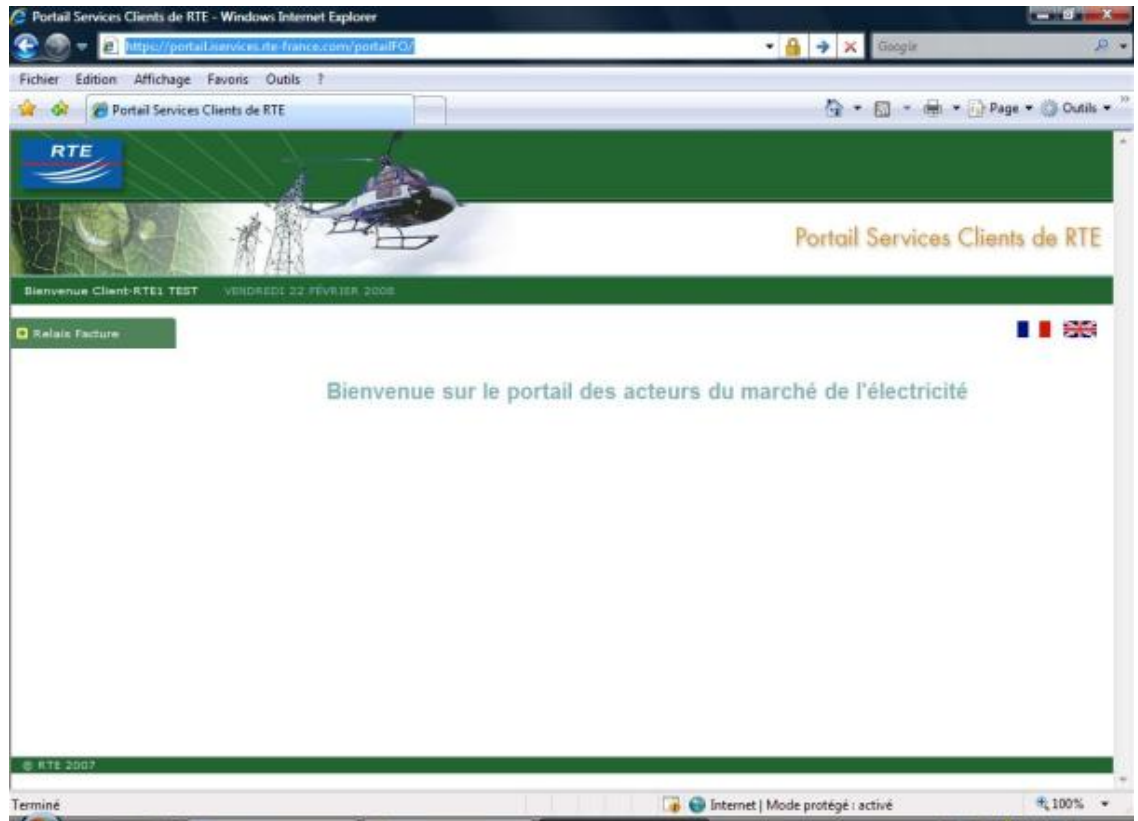
Whenever you access the welcome page with "https" as the prefix, you will have to select your certificate:



The "Display the certificate..." button allows you to look at the contents of the selected certificate, then click on "OK".

If necessary, this window will ask you for the store password for your certificate.

The welcome page will then be displayed in a secure setting:



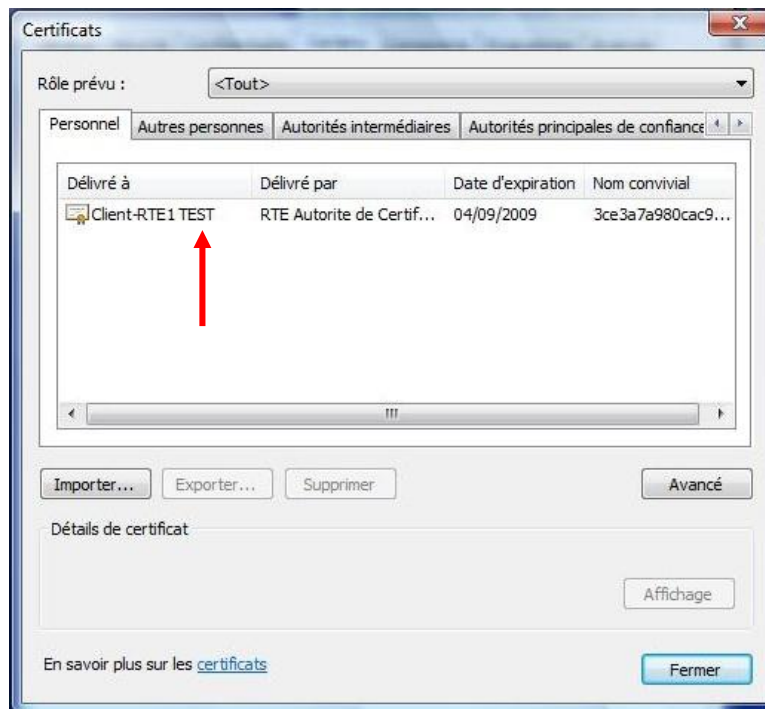
7.6 Supplementary operations

7.6.1 Export of your personal certificate

Under Internet Explorer, export of a certificate with the private key and the root certificate. Once finished, generation of a file in the PKCS#12 (.pfx) format protected with a password.

Under Internet Explorer, open up: « Tools > Internet options... » and click on the "Contents" tab, then on the "Certificates..." button:

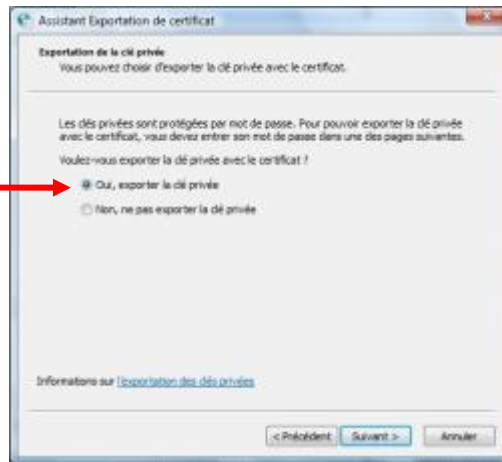
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



Select your certificate, then click on "Export...".

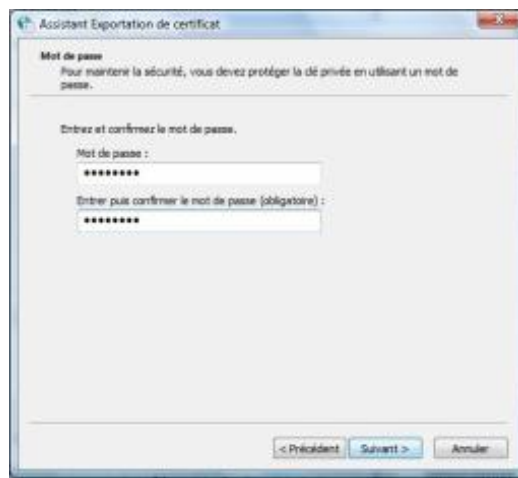
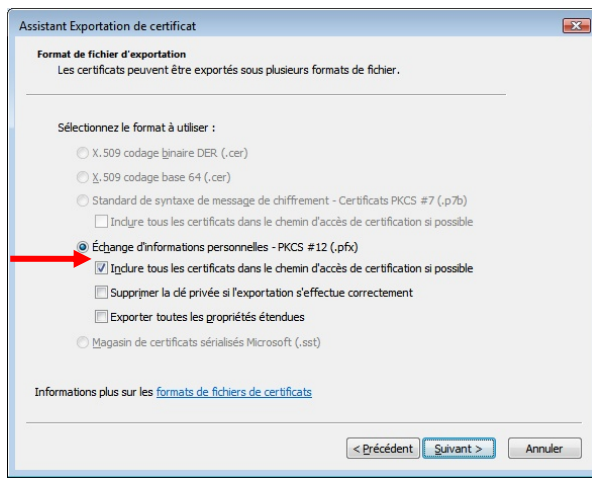


Click on the "Next" button.



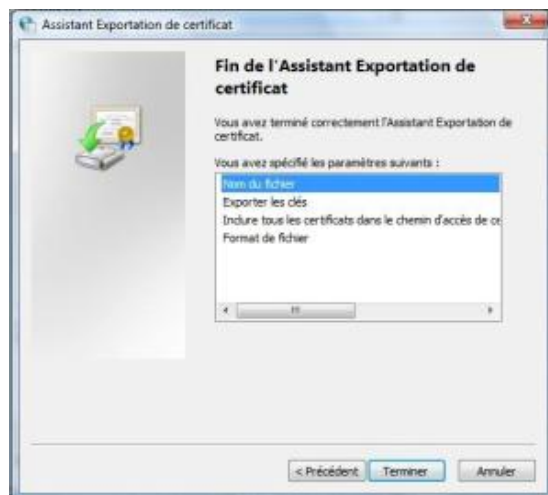
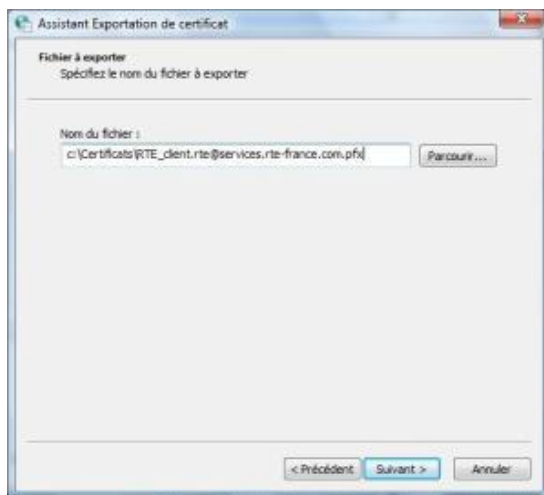
Select "Yes, export the private key", then click on the "Next" button.

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



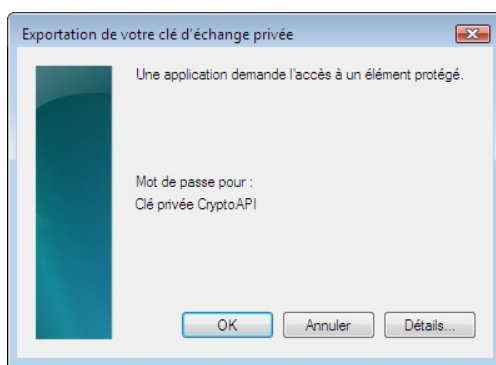
Select the checkbox "Include all certificates in the certification access path where possible", then click on the "Next" button.

Enter a password to restrict access to the PKCS#12 file, then click on "Next".



Enter the name of the PKCS#12 file, then click on the "Next" button.

Lastly, click on the "Finish" button.



Click on "OK".

You have just exported a combination of your certificate, its private key, and the certificate of the CA root into a password protected PKCS#12 standard format file. These elements have therefore been exported, but are still present in the Internet Explorer store.

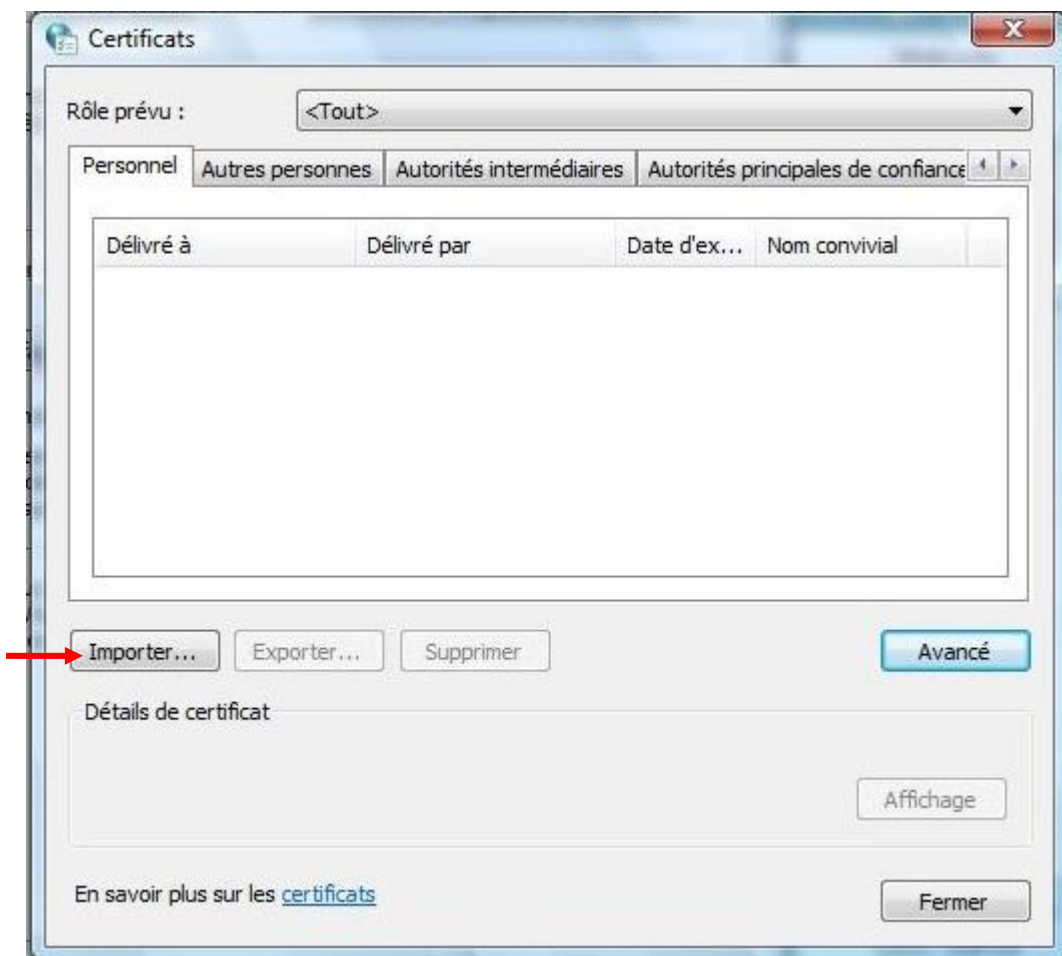
IMPORTANT

Once downloaded, your certificate with its key pair and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to the certificate export procedure §7.6.1.

7.6.2 Import of your personal certificate

With Internet Explorer, import of a password protected PKCS#12 file with the root certificate.

Under Internet Explorer, open up: « Tools > Internet options... » and click on the "Contents" tab, and then on the "Certificates..." button:

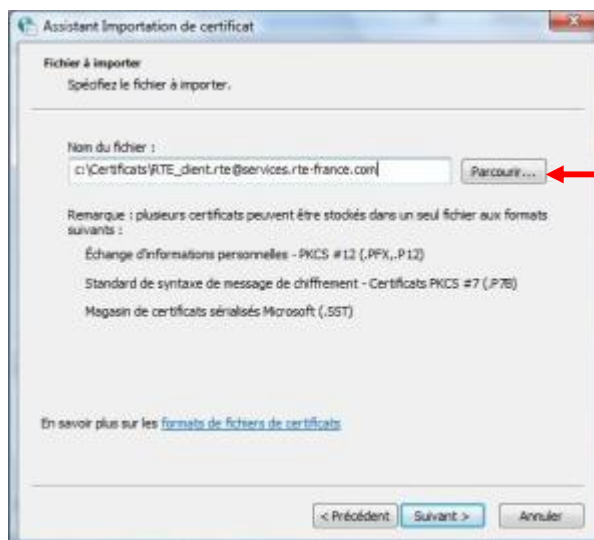


Click on the **"Import"** button.

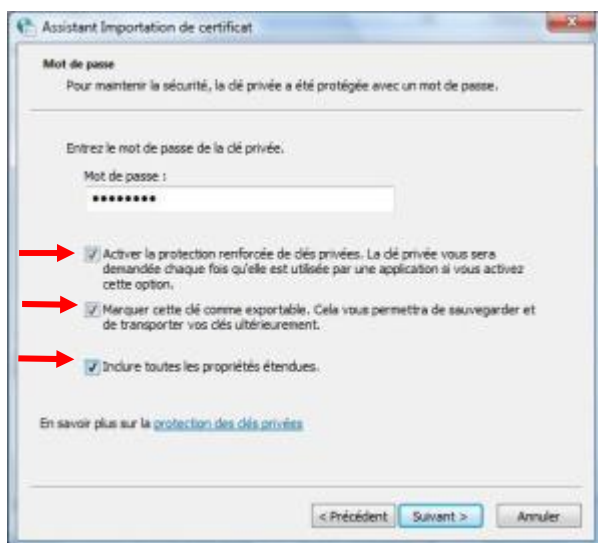
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



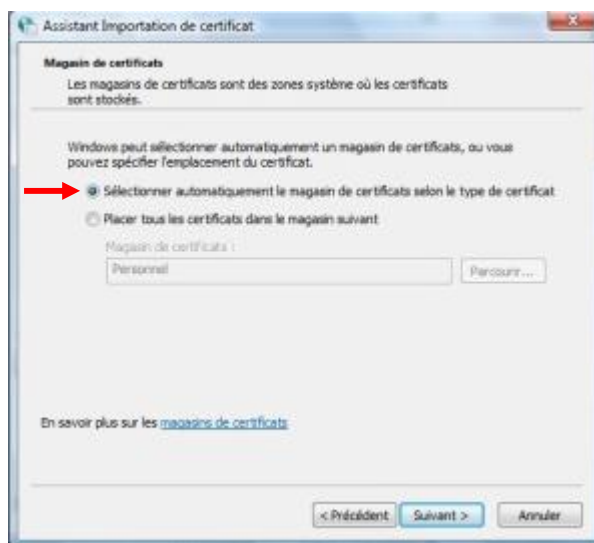
Click on the "Next" button.



Click on the "Browse" button to locate the **PKCS#12 file** (ext. « .p12" or ".pfx"), then click on "Next".

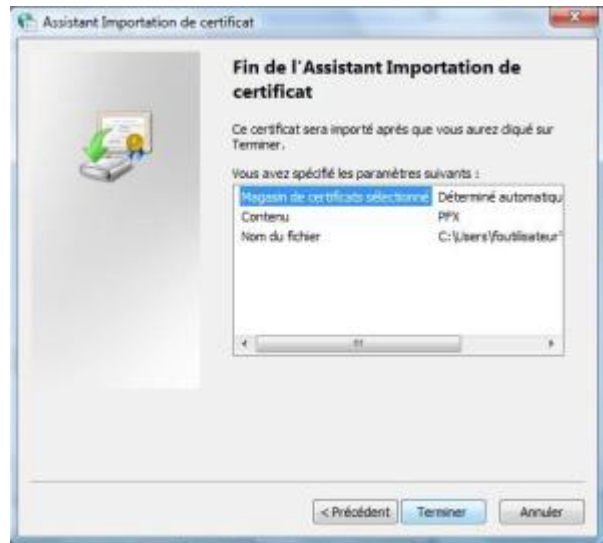


Enter the PKCS#12 file password, check the 3 boxes, then click on "Next".



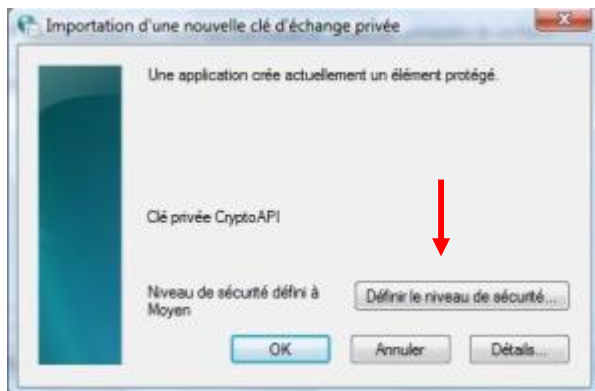
Select the first box, then click on "Next".

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual

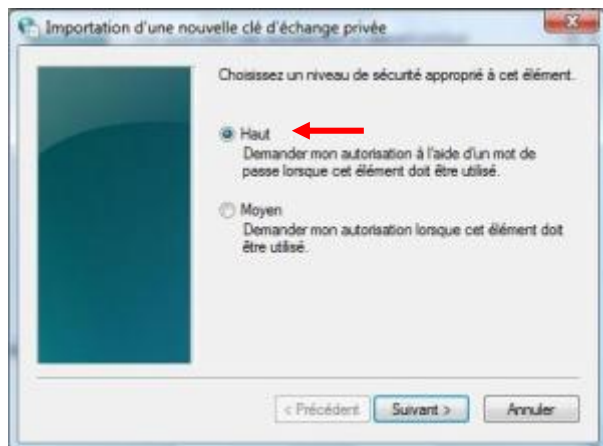


Lastly, click on "**Finish**".

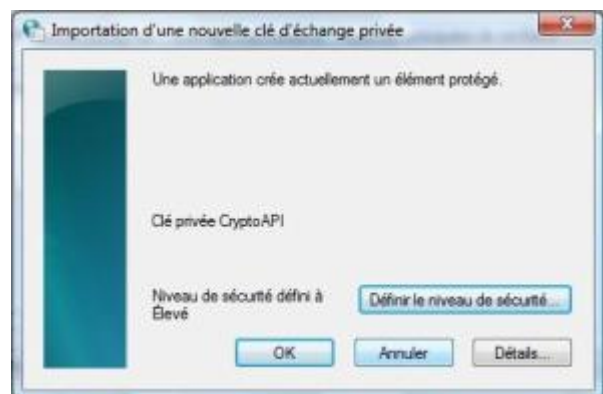
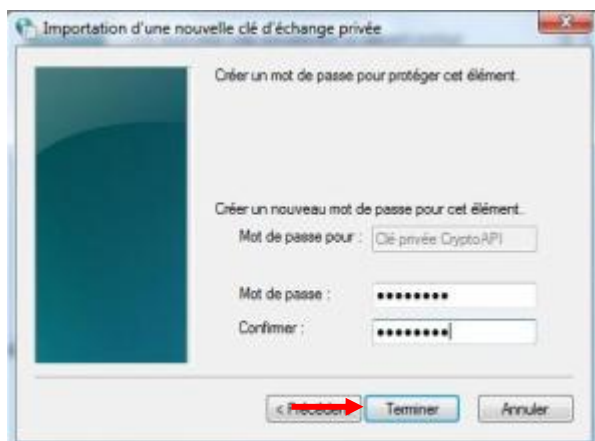
Select the **security level of the private key** that you are importing with the certificate.



Click on the "**Define the security level**" button.

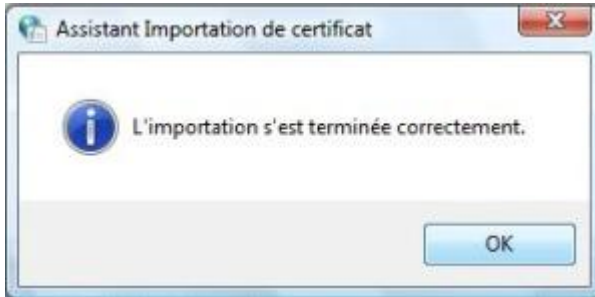


Select the "**High**" option, then click on the "Next" button.



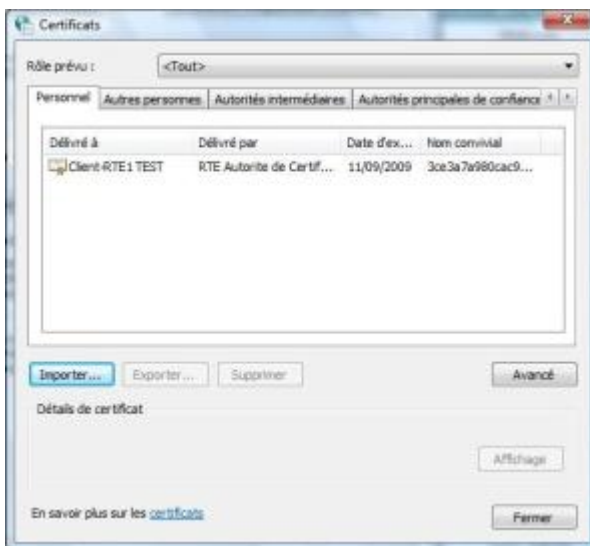
Enter a name for the "key pair" element to protect and a **password**, then click on the **"Finish"** button.

Click on the "OK" button.

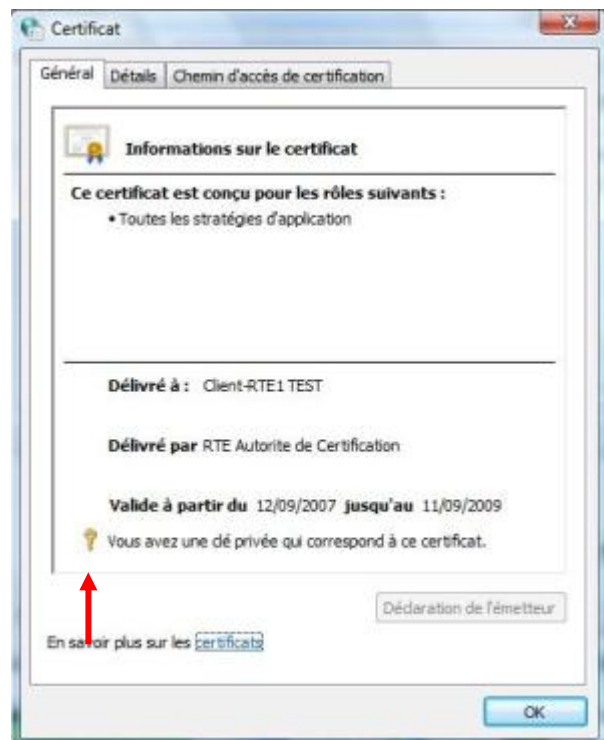


Click on the "OK" button.

Your **certificate**, your **private key** and the **root certificate** of the RTE CA have been imported into Internet Explorer.



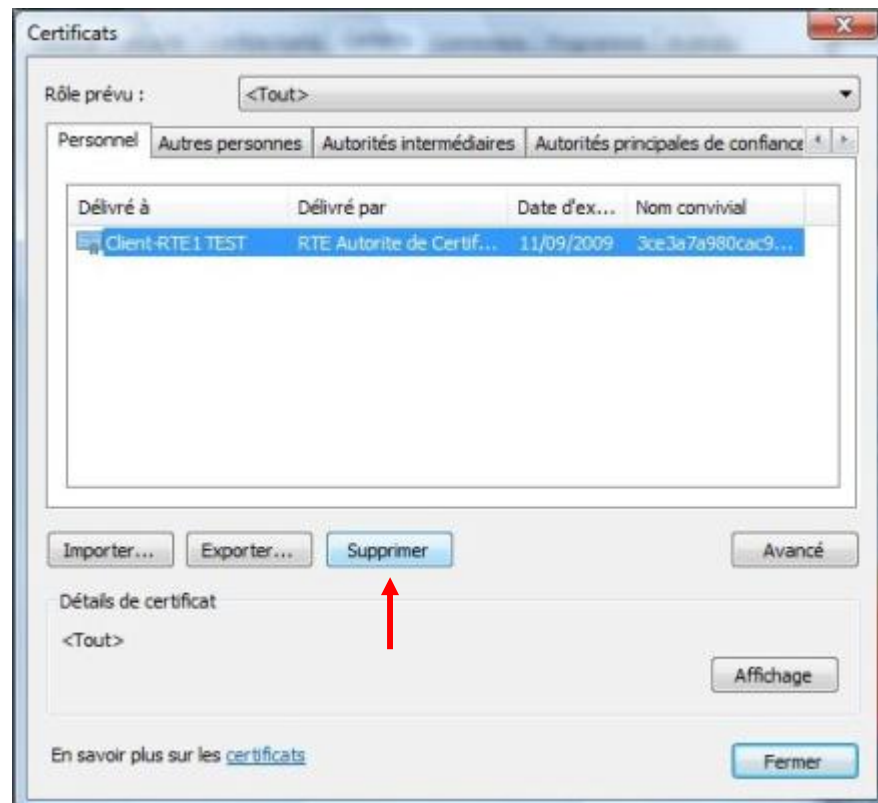
The image on the right shows that the private key is indeed present.



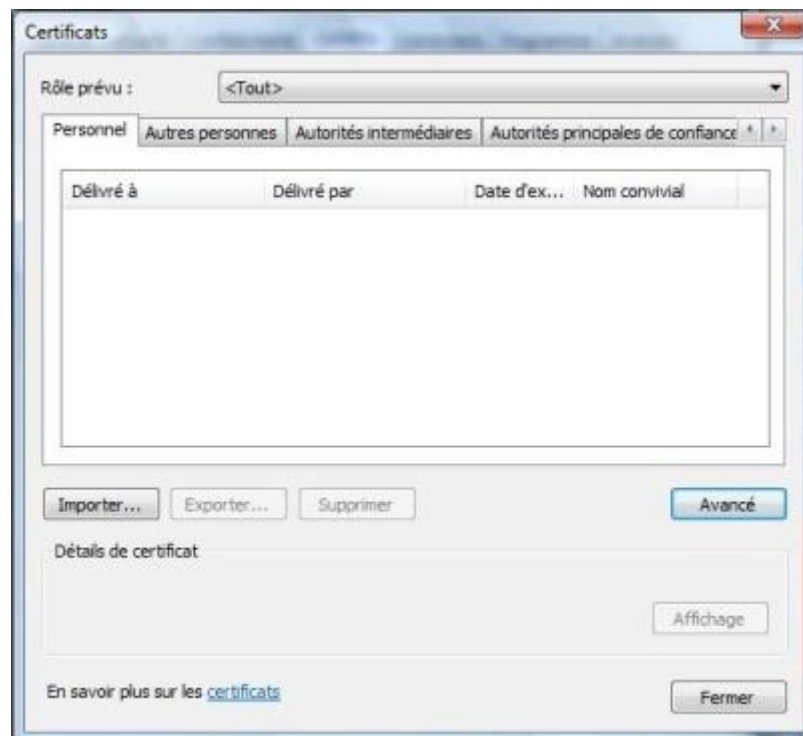
7.6.3 Deletion of your personal certificate

With Internet Explorer, deletion of a certificate with the private key.

Under Internet Explorer, open up: « Tools > Internet options... » and click on the "Contents" tab, and then on the "Certificates..." button:



Select the certificate to be deleted and click on "Delete"



The certificate is deleted from the certificate list.

7.7 Connection to the SSL VPN

7.7.1 Foreword

Connection via SSL VPN is a service which offers the establishment of a secured communications channel to RTE FrontOffice through the Internet. This channel is established after authentication of your certificate with a dedicated site.

The use of SSL VPN requires the installation of a special tool which is installed during your first connection to the site. This application is called **Windows Secure Application Manager (WSAM)**.

The SSL VPN makes it possible to access email folders hosted in RTE FrontOffice.

7.7.2 Prerequisites

The site **secure.iservices.rte-france.com** must be declared as a trusted site (see section §7.2)

IMPORTANT

Before making your first connection, you absolutely must verify that your workstation can resolve the address **secure.iservices.rte-france.com** (see section §6.1.2).

7.7.3 First connection

This paragraph only concerns your first connection to the SSL VPN with Internet Explorer.

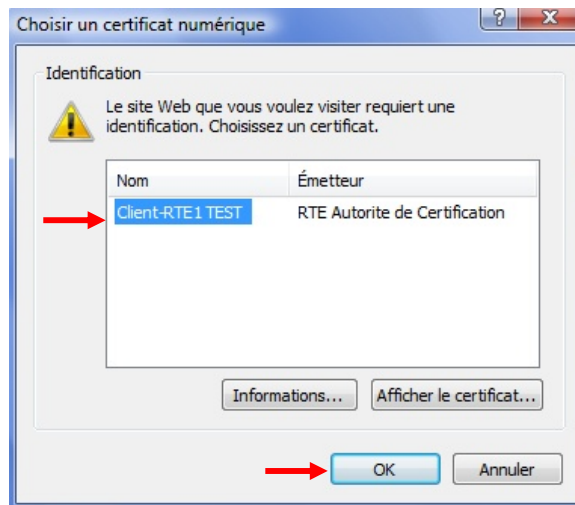
IMPORTANT

The first connection must be made by IT staff with Administrative privileges on your workstation so that the WSAM application installation can be made.

Start your browser and enter the following URL:

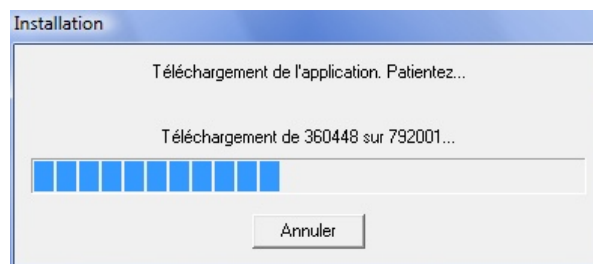
<https://secure.iservices.rte-france.com>

This window will be displayed:



Select your certificate, then click on the "OK" button.

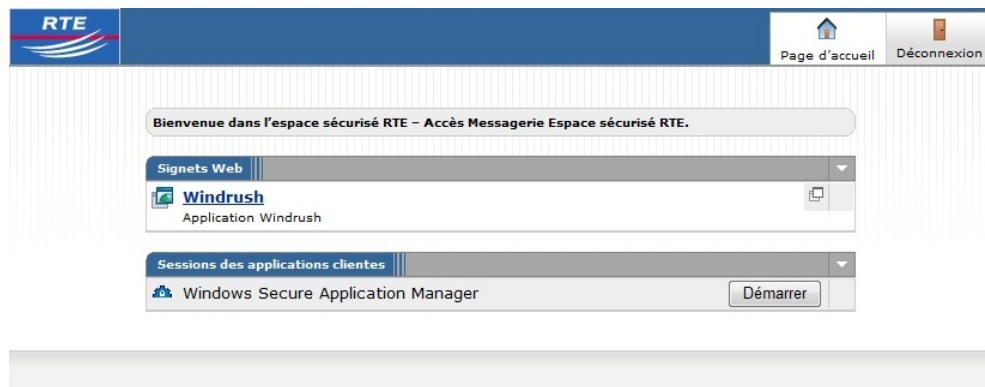
Then the WSAM application installation will start:



Please be patient through the entire installation procedure.

If your Internet access requires authentication with a proxy, a window will appear asking you for your connection identification credentials. Enter them and validate.

Once the installation has completed, the following page will be displayed:



Finally, the  icon will appear in your task bar,

Click on the **Disconnect** button (on the top right of the page) to terminate the session:



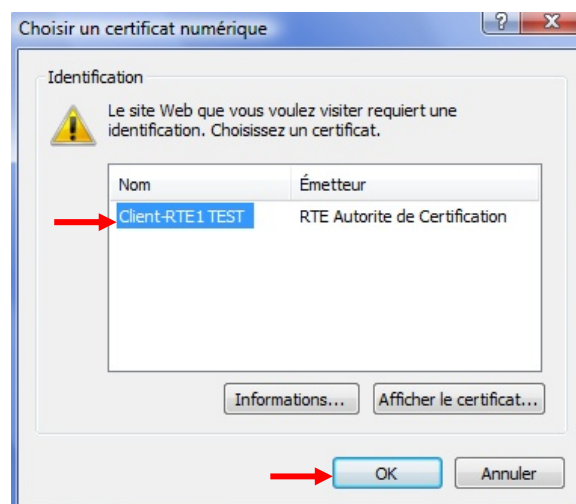
7.7.4 Use of the SSL VPN

7.7.4.1 Establishing the connection

Start your browser and enter the following URL:

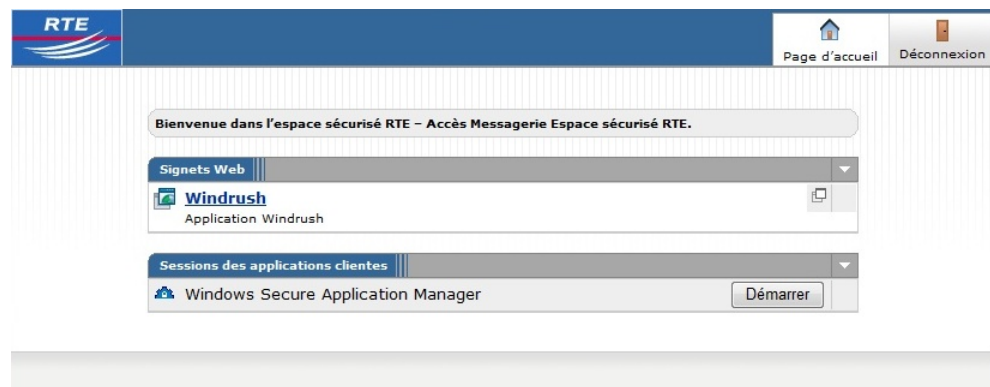
<https://secure.iservices.rte-france.com>

This window will be displayed:



Select your certificate, then click on the "OK" button.

The WSAM application automatically starts and the following page is displayed:



In addition, the  icon will appear in your task bar,

Notes:

- The certificate is only used to establish the SSL VPN connection.
- To close the SSL VPN session, click on the Disconnect button (on the top right of the page).

7.7.4.2 Using SSL VPN to access hosted email folders

SSL VPN can be used to access email folders hosted in FrontOffice with the use of a standard email client.

Access to the hosted email folders requires that the SSL VPN connection has been established (see §7.7.4.1).

The configuration of the email account in your email client software is made in the normal fashion with the following parameters:

- Email server type: POP server
- POP server address: **pop.services.rte-france.com**
- SMTP server address: **smtp.services.rte-france.com**

When your access to RTE FrontOffice is supplied to you, you will receive your login identifier, your password and your email address.

NOTE

Given that the messages are being forwarded through a secure channel, **the sending and receipt of emails does not require the use of a certificate for message encryption.**

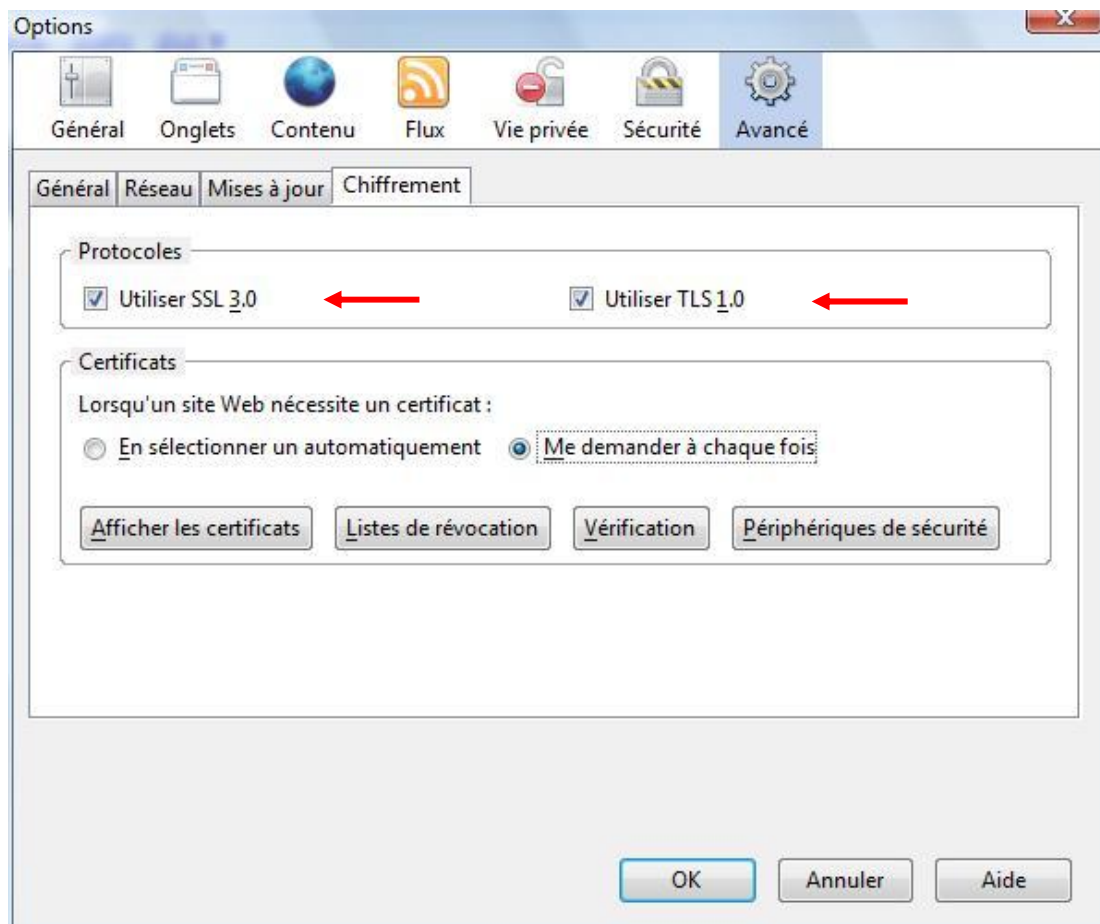
8. Mozilla Firefox



8.1 Preliminary configuration

From the "**Tools > Options...**" menu, select the "**Advanced**" section, and then the "**Encryption**" tab.

In this window, select the 2 checkboxes "Use SLL 3.0" and "Use TLS 1.0":



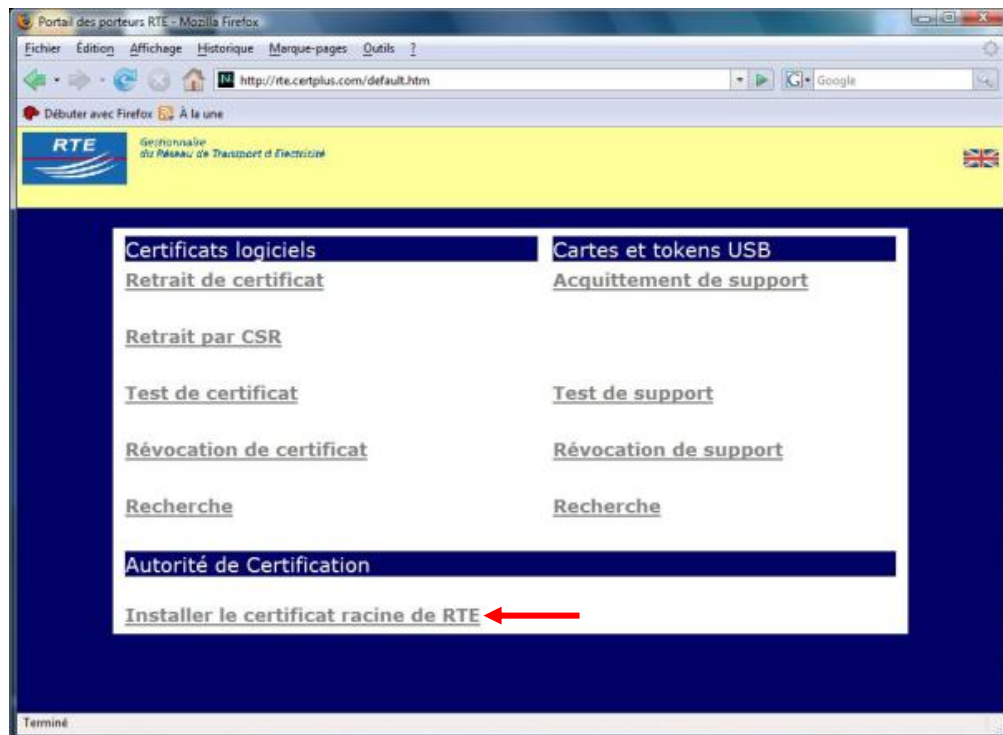
8.2 Installation of the RTE CA root certificate

8.2.1 Download and installation

The RTE root certificate must now be installed in your browser so that RTE is known as the trusted Certification Authority.

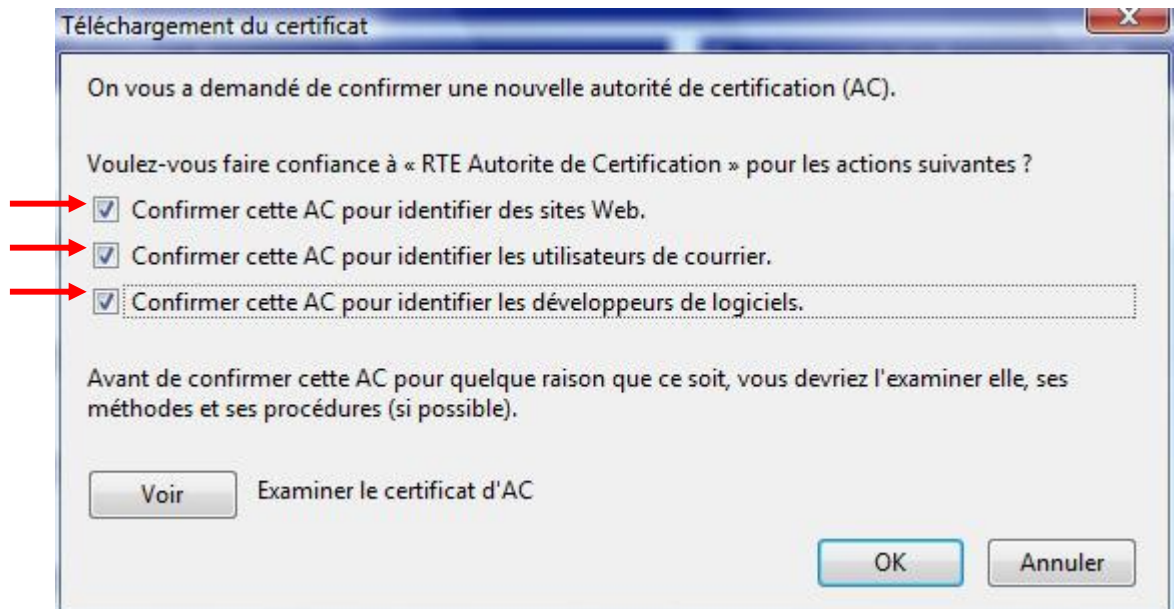
To do this, please navigate to the RTE customer site at the following address:

<http://rte.certplus.com/default.htm>



Click on the link **"Installer le certificat racine de RTE / Install the RTE root certificate"**

A dialogue box will be displayed, in which you must select the 3 checkboxes "Confirm this CA for identification [...]" to confirm confidence in the RTE CA:



8.2.2 Verification of the root certificate fingerprint

Click on **"View"** to verify that the certificate to which you are about to grant trusted status is indeed the RTE root certificate:

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual

To make sure that you have downloaded the genuine RTE AC root certificate, carefully check that the **"SHA1"** or **"MD5"** digital fingerprint displayed in the dialogue box shown is **identical** to that shown opposite.



The **root certificate digital fingerprints** for RTE CA are listed here:

SHA1 A2:9A:4F:A1:77:14:2C:87:FA:30:2D:B0:8F:2C:02:37:37:C7:AE:37

MD5 53:42:6A:2E:A5:10:AB:2A:21:09:EE:88:13:67:A0:31

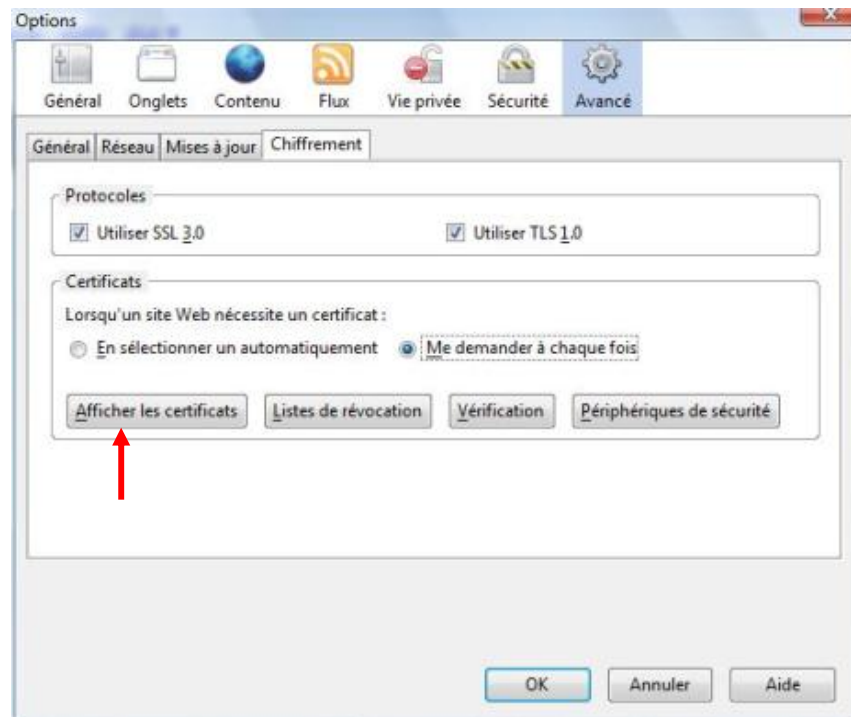
If it is not identical, click on "Close" to return to the previous window where you should click on "Cancel" and contact our support services.

If it is identical, continue the process to finish the import. The "Details" tab:

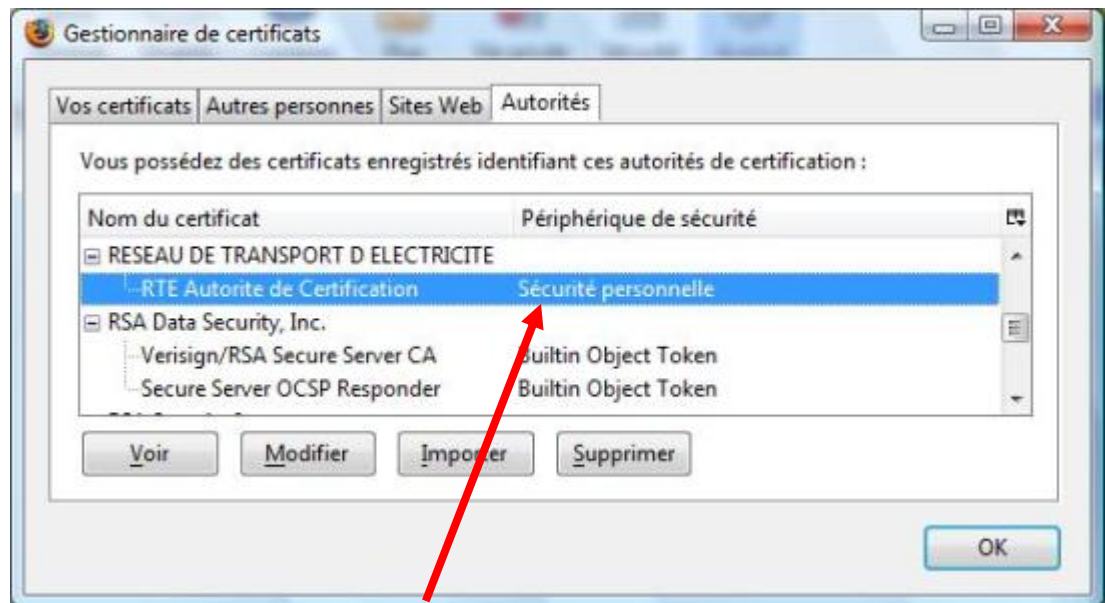


Click on "Close" to return to the initial screen (see above) where you can click on "OK": the RTE CA root certificate is now installed in Mozilla Firefox.

To view this certificate later in Mozilla Firefox, you must use the "Tools > Options..." menu, and select the "Advanced" section and the "Encryption" tab.



Click on the "Display the certificates" button.



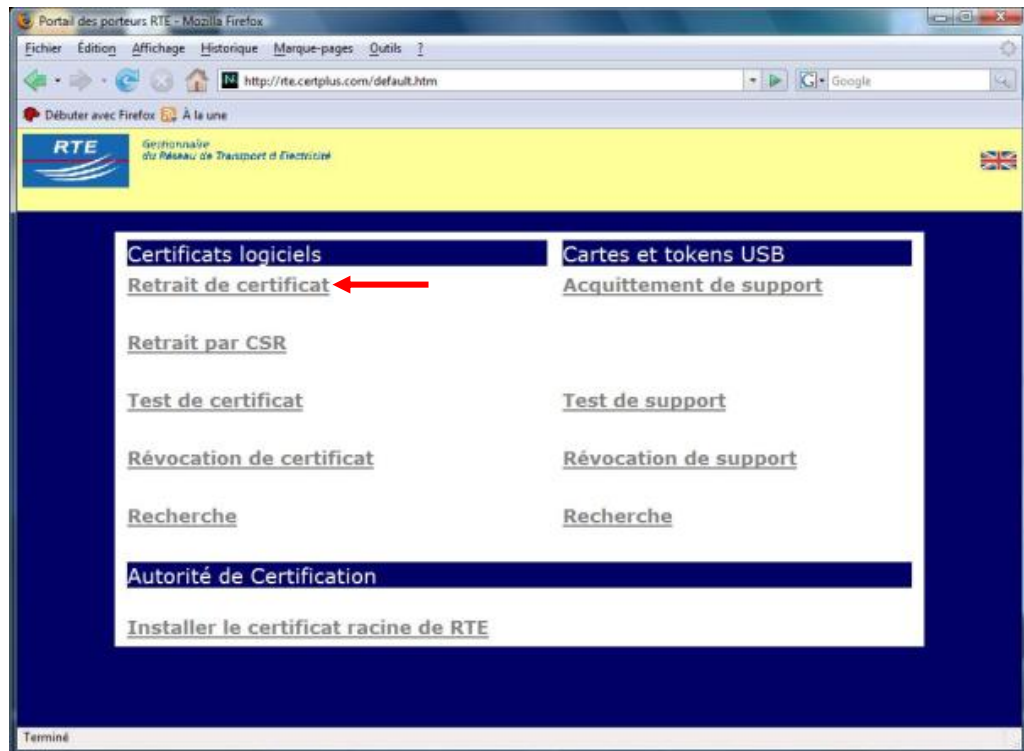
In the "Authorities" tab, you can verify that the "RTE Autorite de Certification" root certificate has indeed been registered on your PC hard drive ("Personal security"), and view it by selecting it and clicking on "View".

8.3 Retrieval of your personal certificate

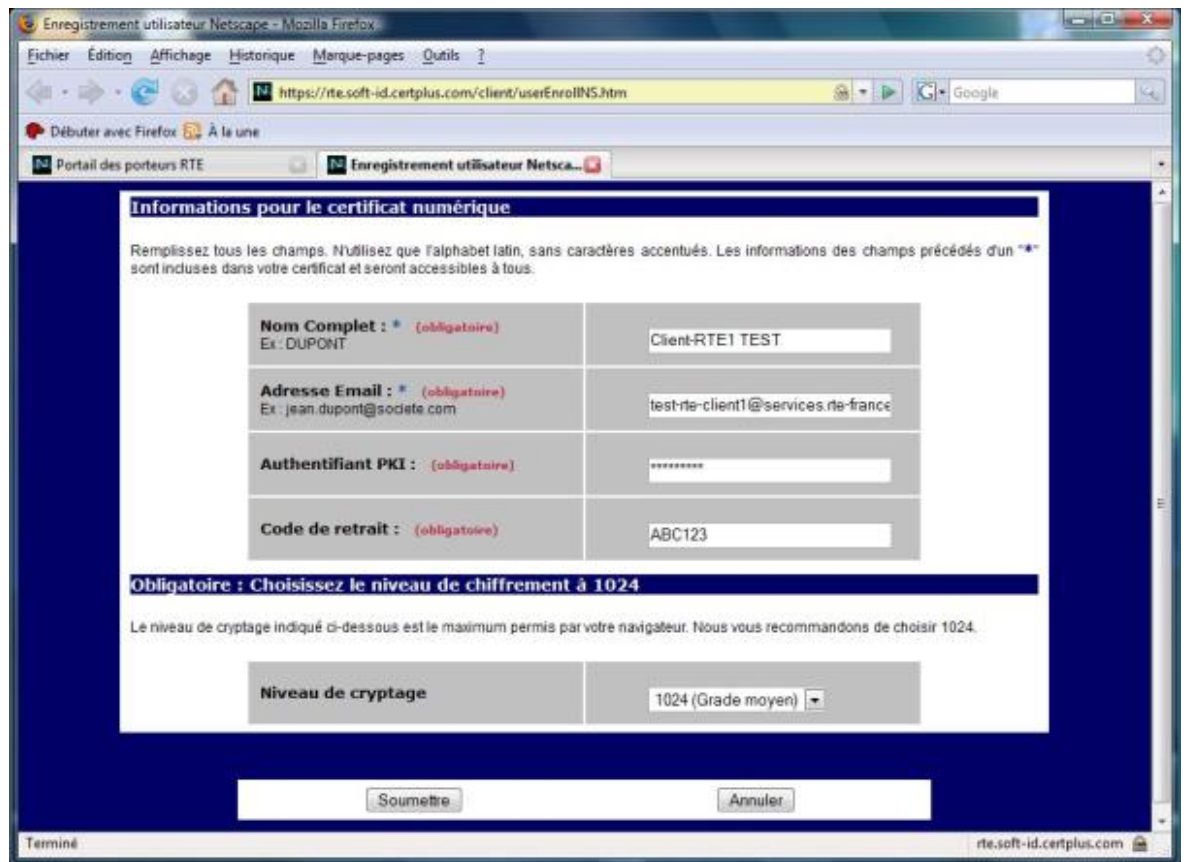
The request for the digital certificate must have been completed as per the procedure laid out in chapter 2

To create your key pair and certificate, you must connect to the following site:

<http://rte.certplus.com/default.htm>



Click on the "**Retrait de certificat / Retrieve the certificate**" button to install your digital certificate.



Enregistrement utilisateur Netscape - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

https://rte.soft-id.certplus.com/client/userEnrollINS.htm

Débuter avec Firefox À la une

Portail des porteurs RTE Enregistrement utilisateur Netsca...

Informations pour le certificat numérique

Remplissez tous les champs. N'utilisez que l'alphabet latin, sans caractères accentués. Les informations des champs précédés d'un "*" sont incluses dans votre certificat et seront accessibles à tous.

Nom Complet : * (obligatoire) Ex : DUPONT	Client-RTE1 TEST
Adresse Email : * (obligatoire) Ex : jean.dupont@sodete.com	test-rte-client1@services.rte-france
Authentifiant PKI : (obligatoire)	*****
Code de retrait : (obligatoire)	ABC123

Obligatoire : Choisissez le niveau de chiffrement à 1024

Le niveau de cryptage indiqué ci-dessous est le maximum permis par votre navigateur. Nous vous recommandons de choisir 1024.

Niveau de cryptage	1024 (Grade moyen)
---------------------------	--------------------

Soumettre Annuler

Terminé rte.soft-id.certplus.com

The fields marked with an asterisk must be completed **without diacritic marks** (i.e. accents, cedillas, ...) **or punctuation marks**; as they would also appear in the certificate that will be generated.

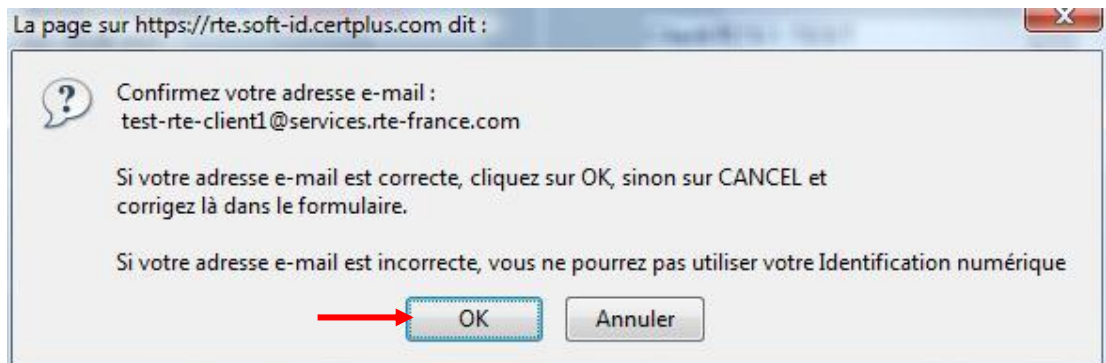
The **retrieval code** is the code supplied in the 2nd email that you received from us which allows you to authenticate yourself. To make things easier, you can do simple copy-paste commands to enter the data.

You must likewise enter your **Authentifiant Utilisateur PKI (PKI User Credentials)**, just as they were supplied in the RTE IT system access technical specifications; they will serve to authenticate you with the RTE Hotline any time that you contact them.

On this form, a dropdown list directly asks you to select the key size. You **absolutely** must select a size of **1024 bits**.

Lastly, click on "**Submit**" to send your request for the digital certificate.

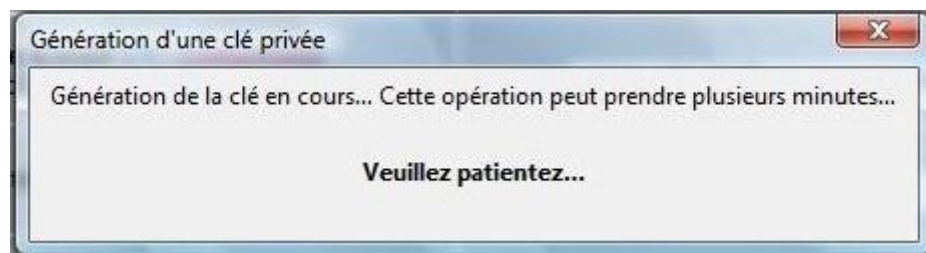
A dialogue box will ask you to confirm your email address:



Click on "OK".

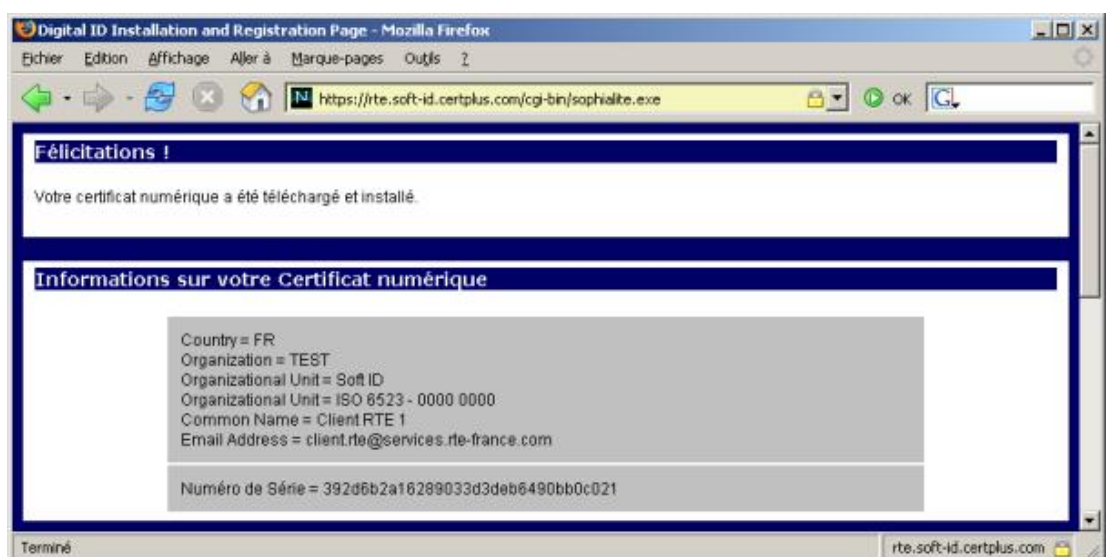
8.3.1 Generation of the key pair

Finally, the RSA key pair is generated by Mozilla Firefox, and the following message is displayed:



8.3.2 Installation of the certificate

Your certificate is finally downloaded and installed in the Mozilla Firefox certificate store. The following page will then be displayed to indicate the end of the process:



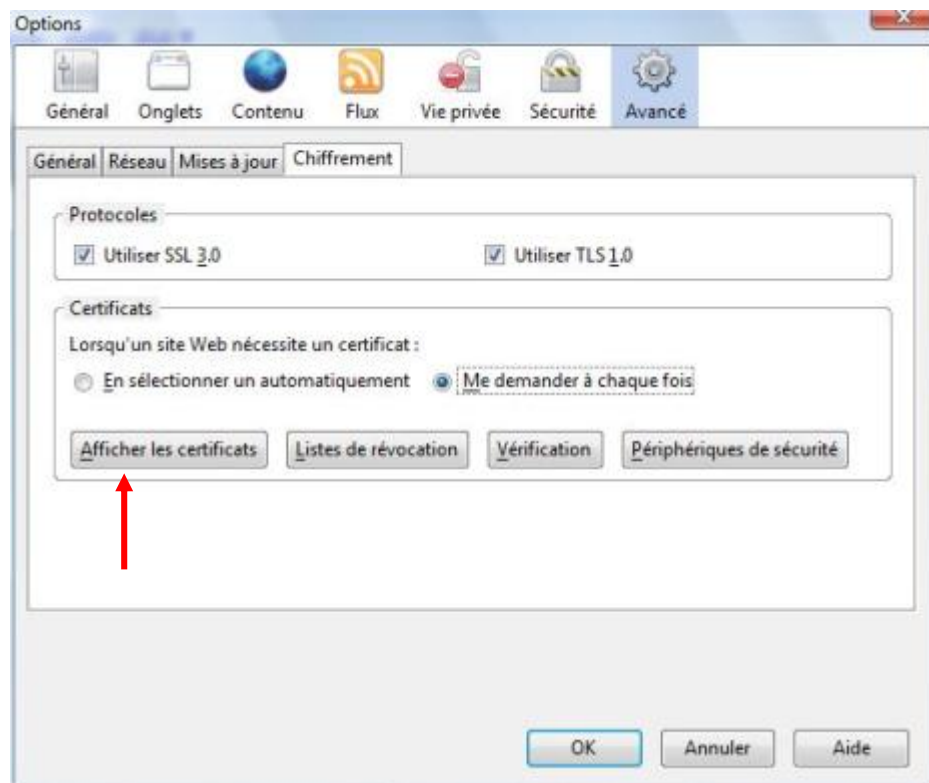
IMPORTANT

Once downloaded, your certificate with its keys and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to section §8.5.1 for the certificate export procedure.

8.3.3 Viewing and verification of your digital certificate

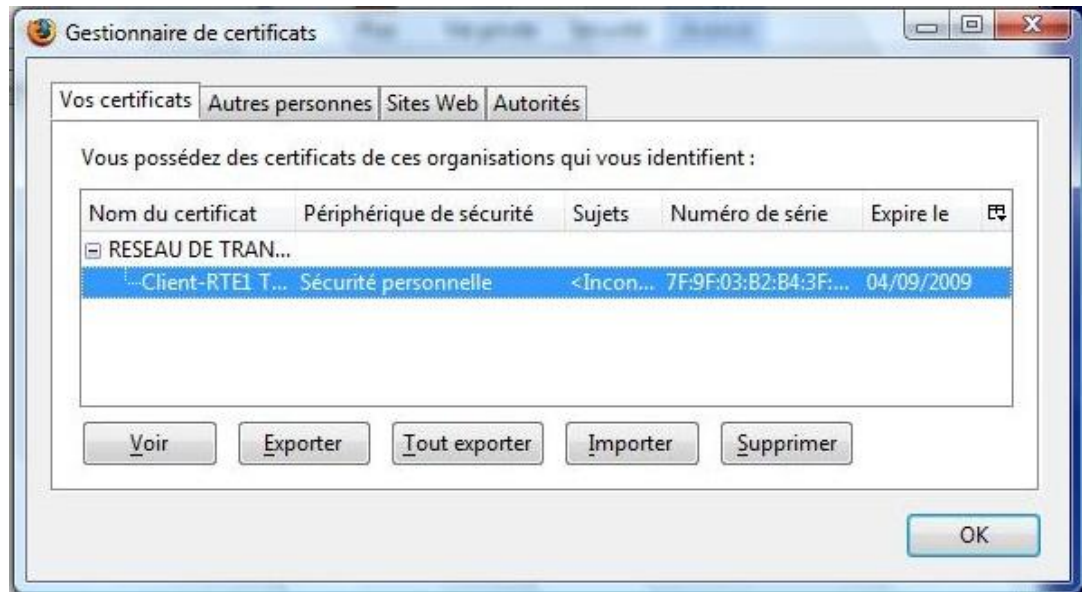
Regardless of the browser used, the contents of the downloaded certificate will obviously be the same, only the presentation of the information on the screen will vary.

For Mozilla Firefox, you must click on the **"Advanced"** section, and then on the **"Encryption"** tab:



Click on the **"Display the certificates"** button.

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



The "Your certificates" tab.

The certificate is a digital certificate: once installed, it will be described as "Personal security". You can view it by selecting it and clicking on "View".



Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



The 1st tab displays the message "This certificate has been verified for the following uses". The 2nd tab displays the certification hierarchy with the RTE CA root certificate. This ensures that all the certificates have been correctly installed, and that all the correct usage conditions for your certificate have been satisfied.

8.4 Use of your certificate

8.4.1 Authentication and encryption

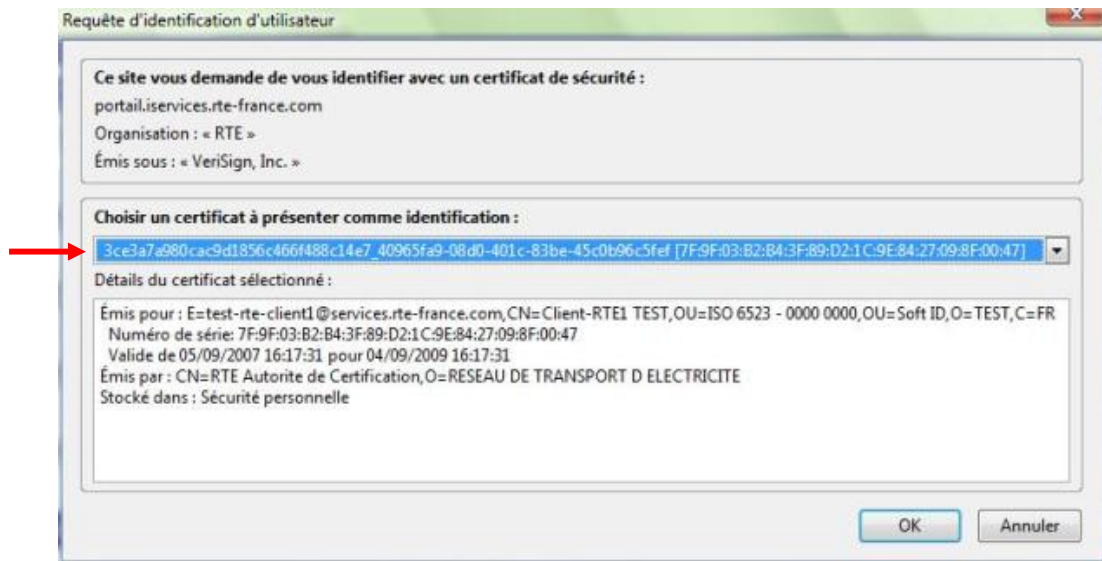
Steps to follow:

- Start Mozilla Firefox;
- Enter the URL for the RTE application or for the "RTE Customer Services Portal" (this URL starts with "https://");
- During authentication, the browser will ask you to choose the certificate before attempting to authenticate you, and then prompt for the certificate store security password;
- If several certificates are offered to you, you should choose the one that was supplied to you for the application which you are currently attempting to access (the contents of the selected certificate from the dropdown list is displayed beneath the list);
- Now all the data that you send and receive will be encrypted.

8.4.2 Example of accessing the "RTE Customer Services Portal"

Whenever you access the welcome page with "https" as the prefix, you will be requested to select your certificate:

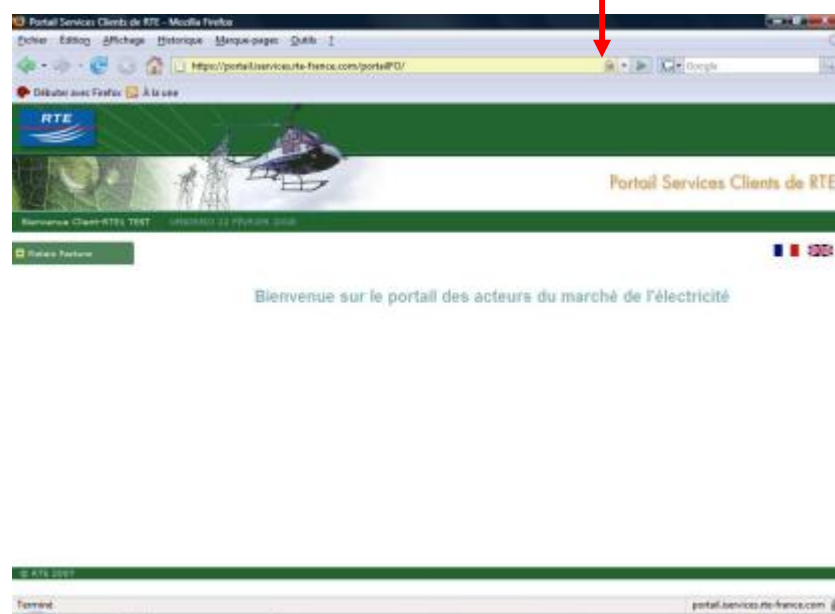
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



Select your certificate from the dropdown list labelled "Choose a certificate to present as identification" and click on "OK". If necessary, this window will ask you for the password to the Mozilla Firefox certificate store.



The welcome page will then be displayed in a secure setting:

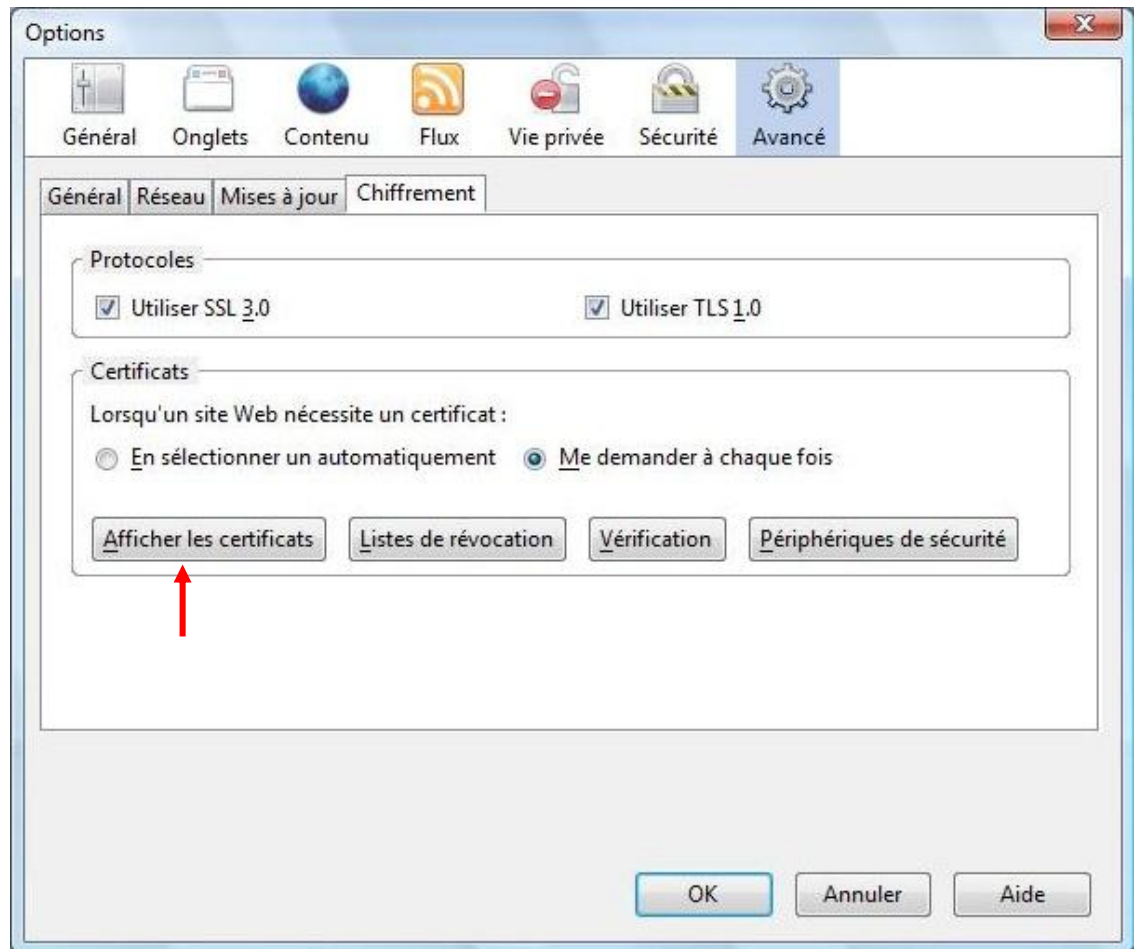


8.5 Supplementary operations

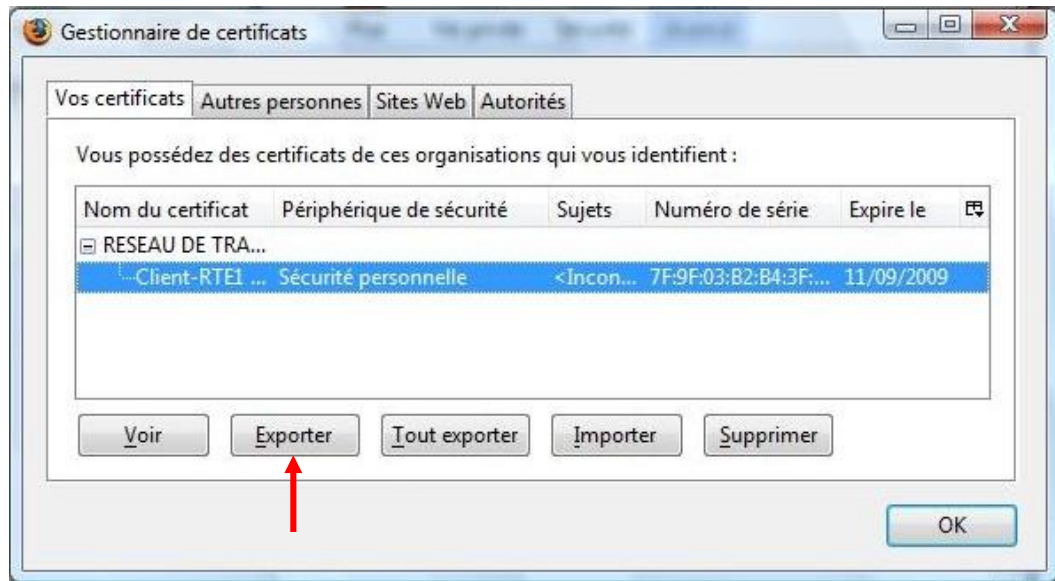
8.5.1 Export of your personal certificate

Under Mozilla Firefox, export of a certificate with the private key and the root certificate. Once finished, generation of a file in the PKCS#12 (.p12) format protected with a password.

From the "Tools > Options..." menu (version 1.5 and higher):

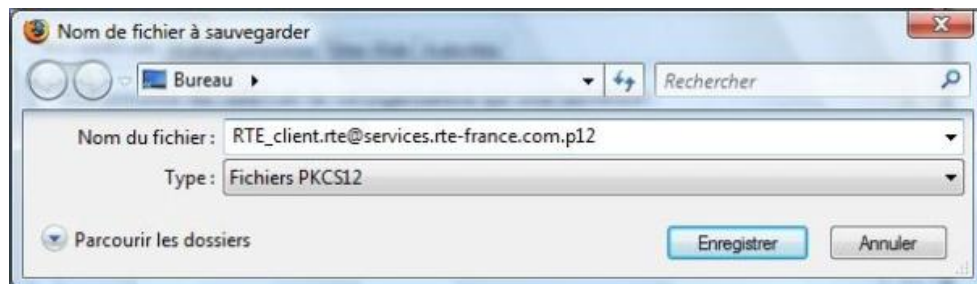


Select "Advanced" > "Encryption", and click on "Display the certificates".



Select your certificate and click on "Export".

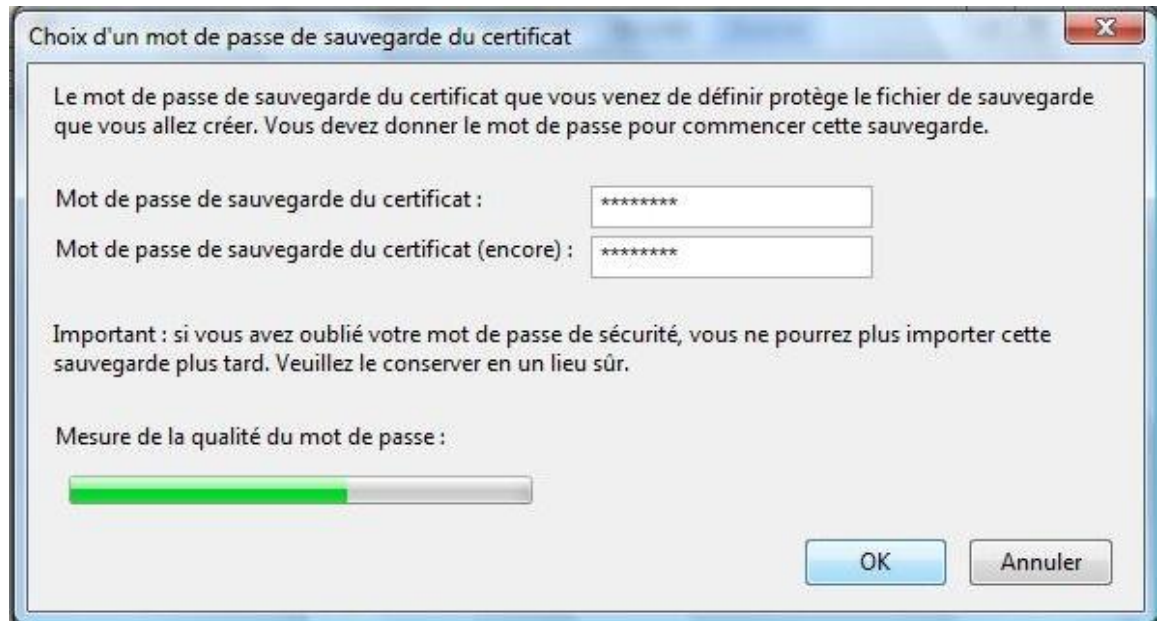
Choose a location and a name for the generated file in the PKCS#12 (.p12) format:



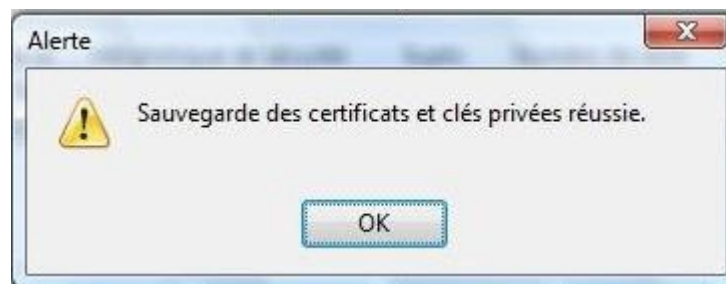
Click on the "Save" button.

If necessary, this window will ask you for the password to the Mozilla Firefox certificate store:





Enter a password to restrict access to the PKCS#12 (.p12) file, then click on "OK".



Your certificate, your private key, and the CA root certificate are exported to the generated file with the ". p12" extension.

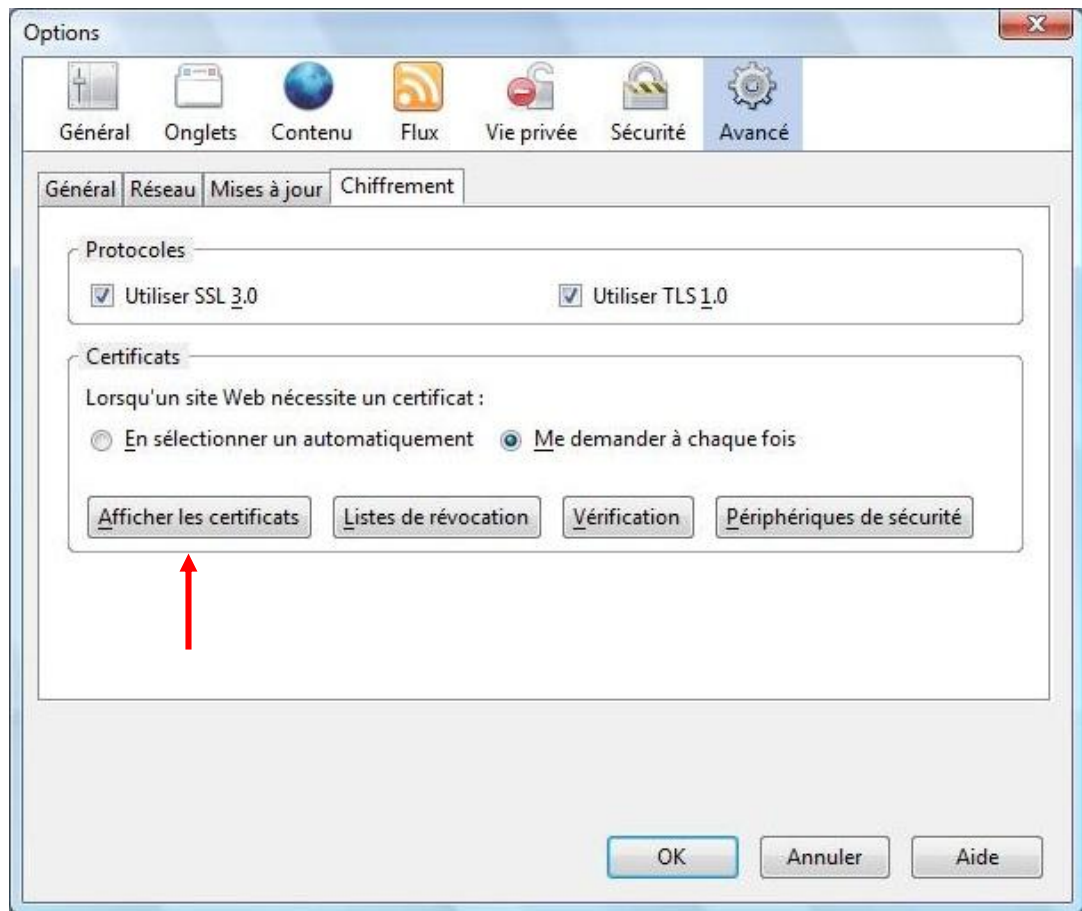
IMPORTANT

Once downloaded, your certificate with its key pair and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to the certificate export procedure.

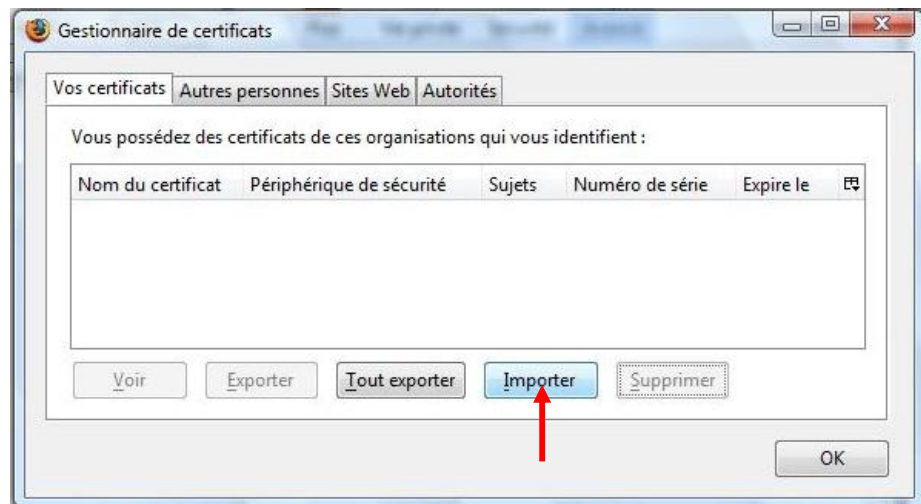
Import of your personal certificate

With Mozilla Firefox, import of a complete PKCS#12 file with the root certificate.

In the "Tools > Options..." menu, select the "Advanced" section and the "Security" tab (v. 1.5 and higher):

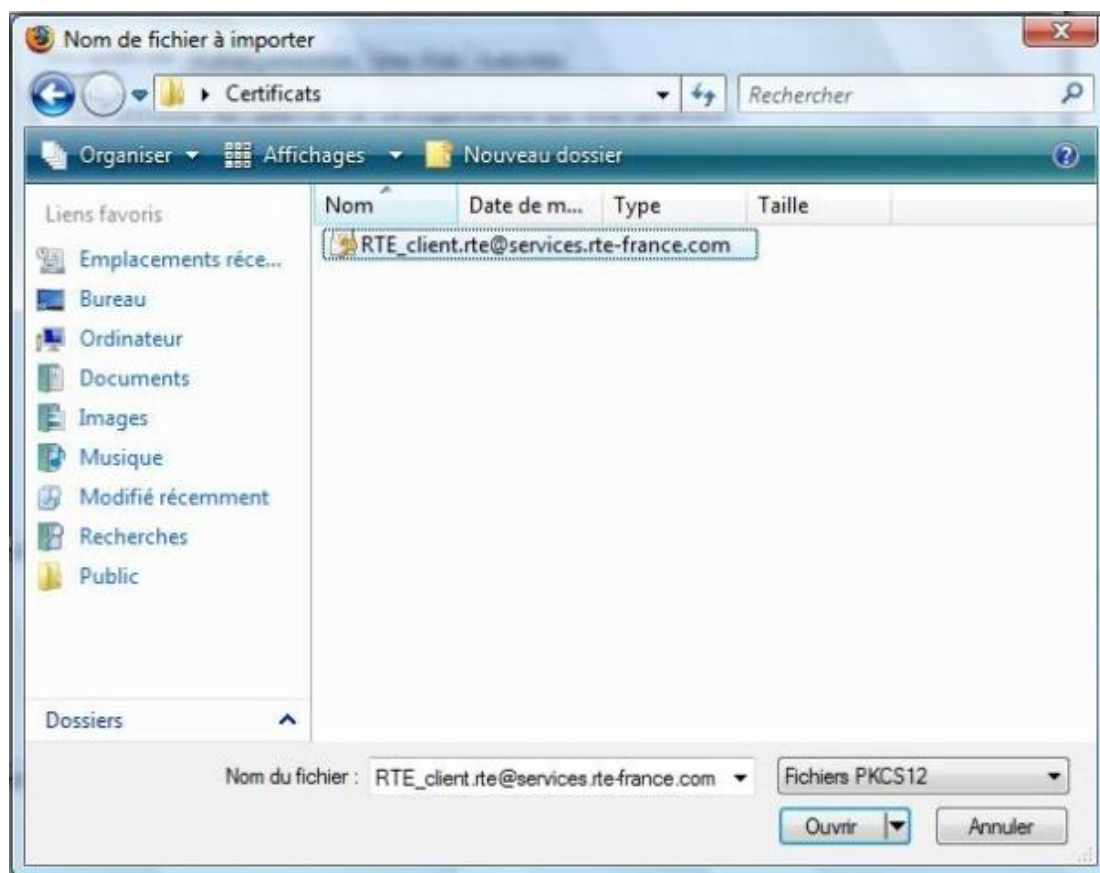


Click on "Display the certificates".



Click on "Import".

Select the PKCS#12 file (with a ".p12" or ".pfx" extension):



Enter the password to access the Mozilla Firefox certificate store:

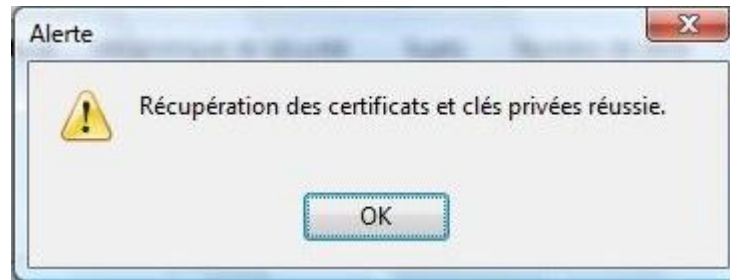


Click on "OK".

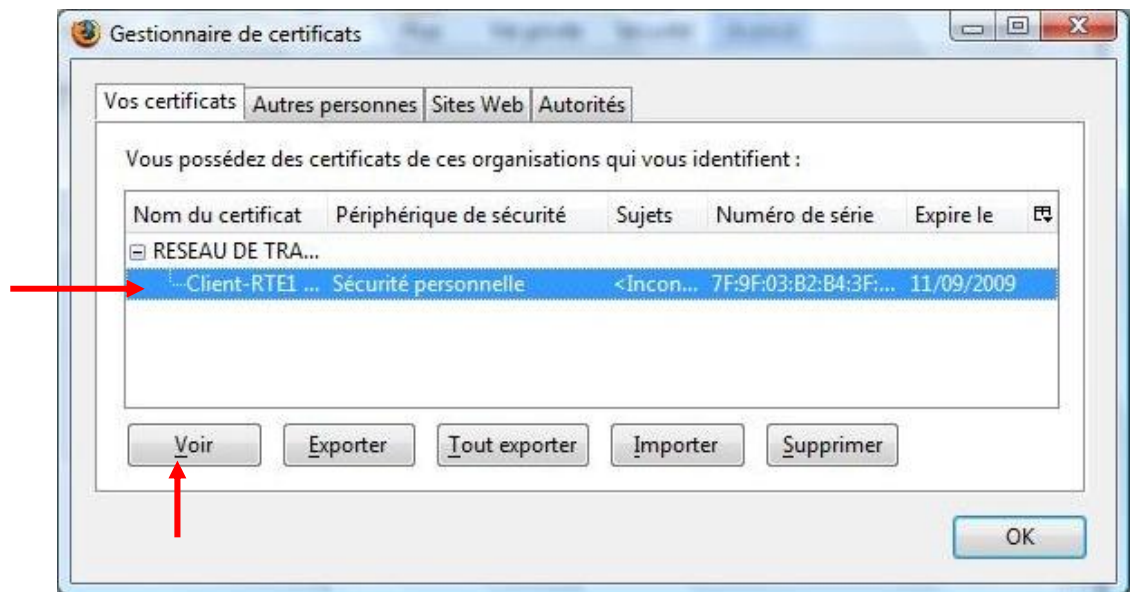


Enter the password restricting access to the PKCS#12 file, then click on "OK".

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



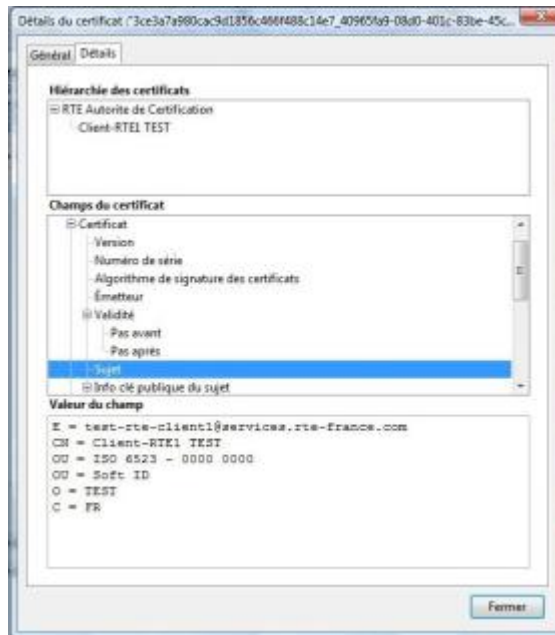
Your certificate is now in the Mozilla Firefox certificate store.



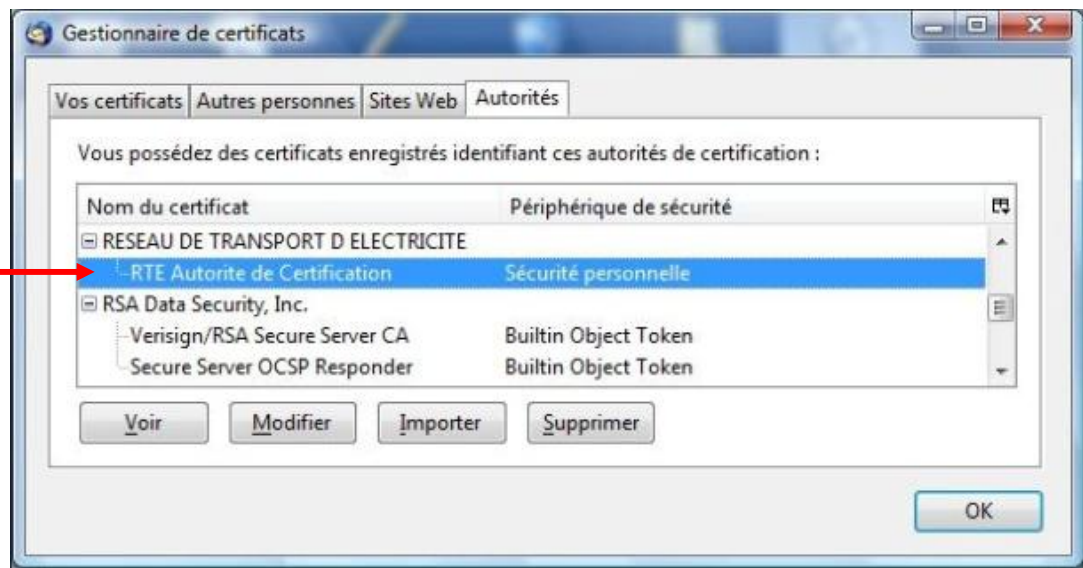
Check that it's the right one by clicking on the "View" button.



Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



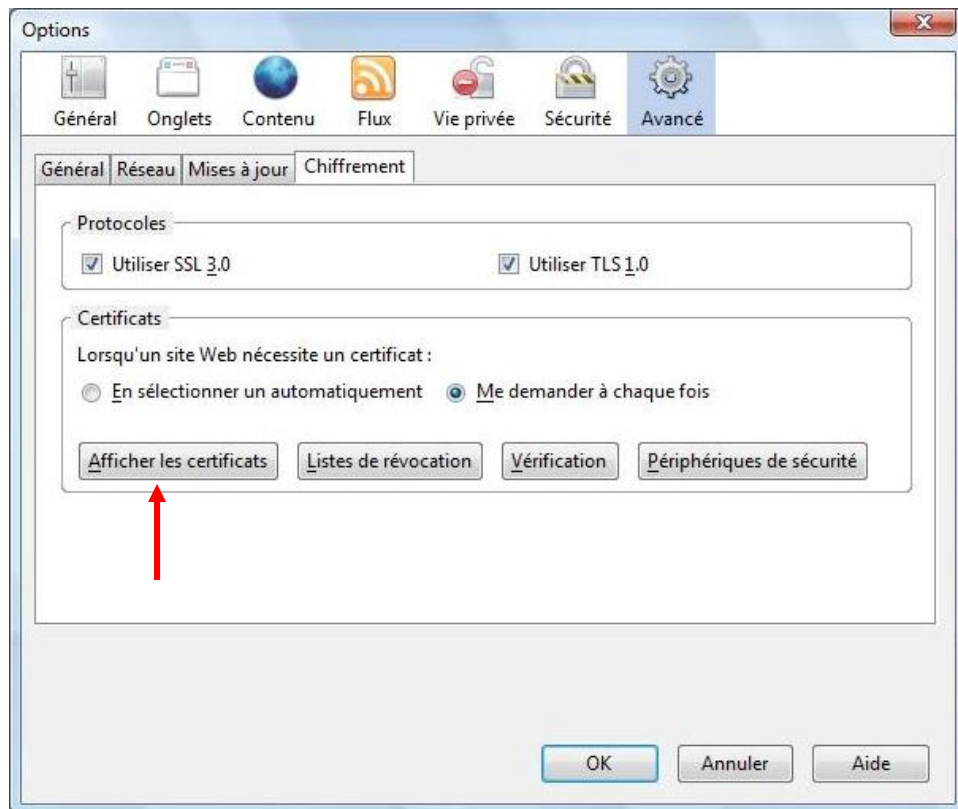
The RTE CA certificate is also in the Mozilla Firefox store:



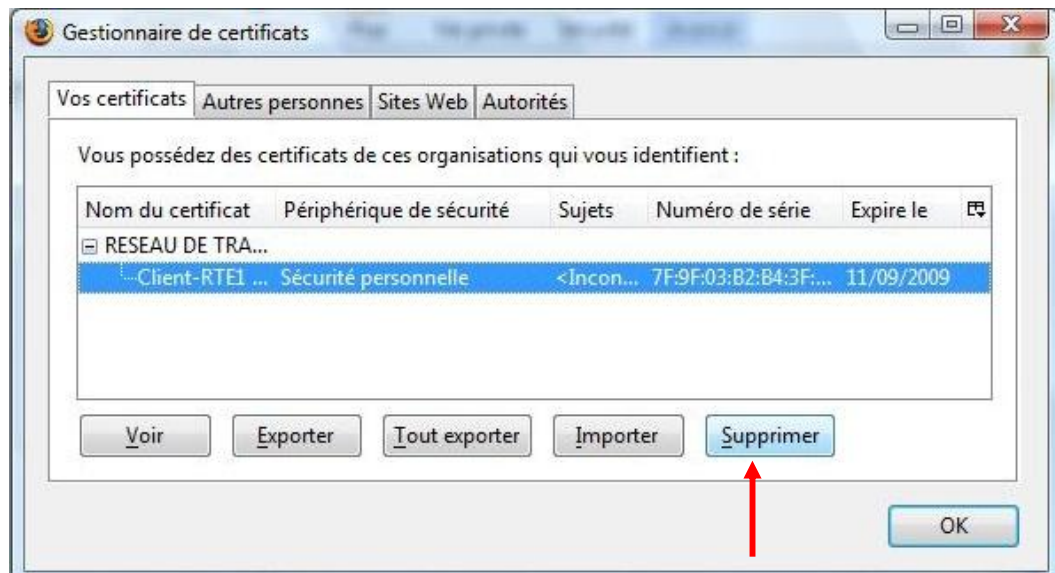
8.5.2 Deletion of your personal certificate

With Mozilla Firefox, deletion of a certificate with the private key.

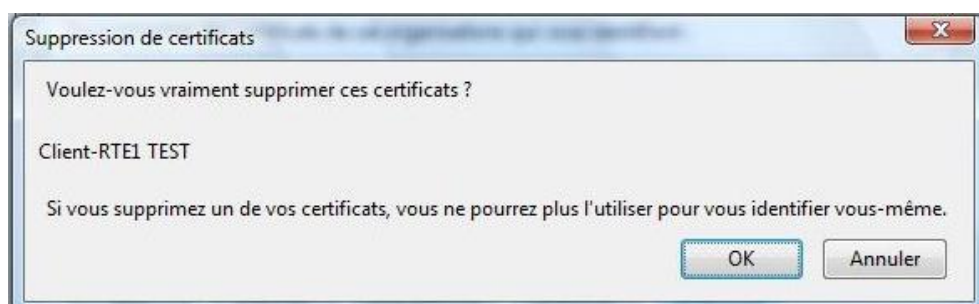
In the "Tools > Options..." menu, select the "Advanced" section and the "Security" tab (v. 1.5 and higher):



Click on "Display the certificates".

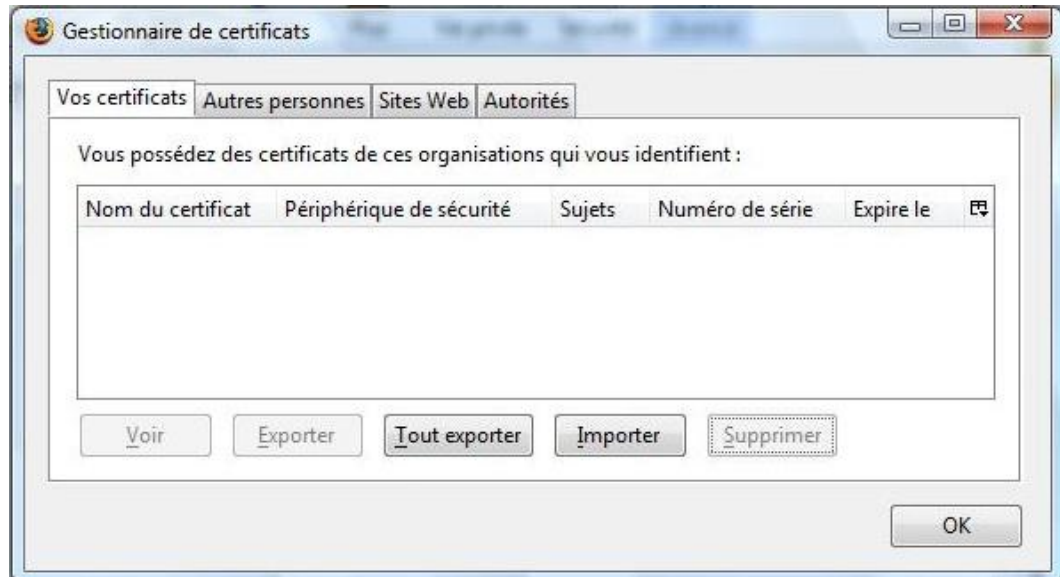


Click on "Delete"



Click on the "OK" button.

The certificate is now deleted from the certificate list.



8.6 Connection to the SSL VPN

8.6.1 Foreword

Connection via SSL VPN is a service which offers the establishment of a secured communications channel to RTE FrontOffice through the Internet. This channel is established after authentication of your certificate with a dedicated site.

The use of SSL VPN requires the installation of a special tool which is installed during your first connection to the site. This application is called **Windows Secure Application Manager (WSAM)**.

The SSL VPN makes it possible to access email folders hosted in RTE FrontOffice.

8.6.2 Prerequisites

First verify that your version of Mozilla Firefox permits access to the RTE's SSL VPN (see §6.2)

IMPORTANT

Before making your first connection, you absolutely must verify that your workstation can resolve the address **secure.iservices.rte-france.com** (see section §6.1.2).

8.6.3 First connection

This paragraph only concerns your first connection to the SSL VPN with Mozilla Firefox.

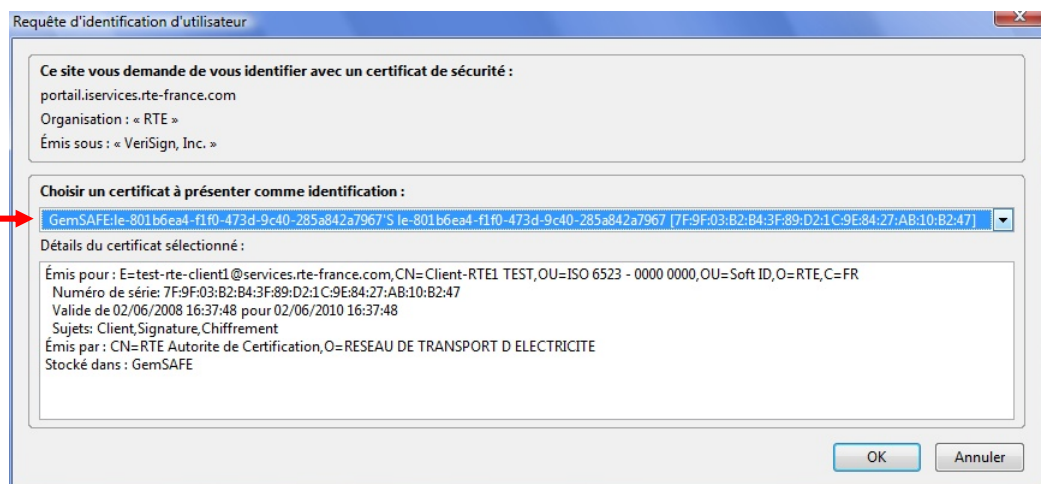
IMPORTANT

The first connection must be made by IT staff with Administrative privileges on your workstation so that the WSAM application installation can be made.

Start your browser and enter the following URL:

<https://secure.iservices.rte-france.com>

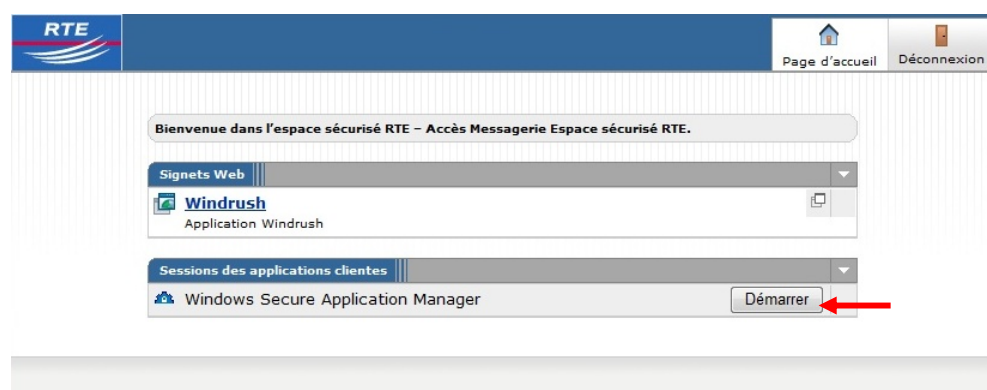
This window will be displayed:



Select your certificate from the dropdown list labelled "Choose a certificate to present as identification" and click on "OK". If necessary, this window will ask you for the password to the Mozilla Firefox certificate store.



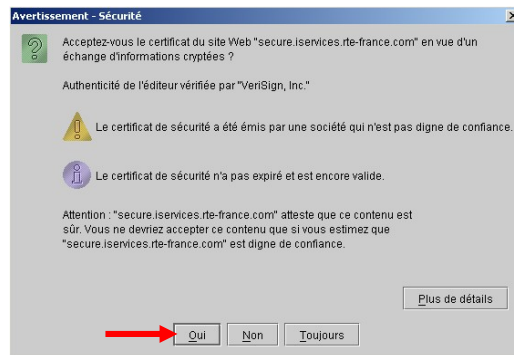
Then the following page will be displayed:



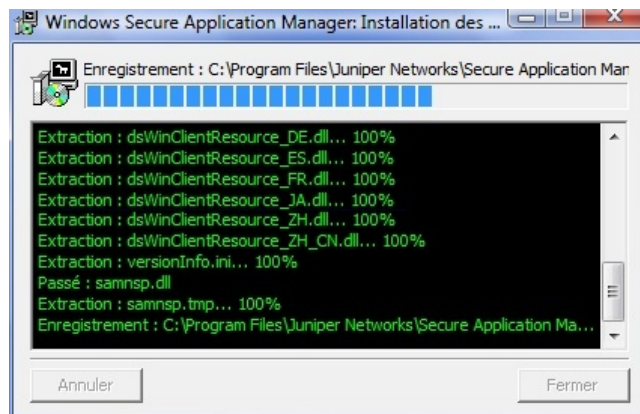
Click on the **"Start"** button to commence the installation.

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual

If this window below appears, just click on **Yes**.

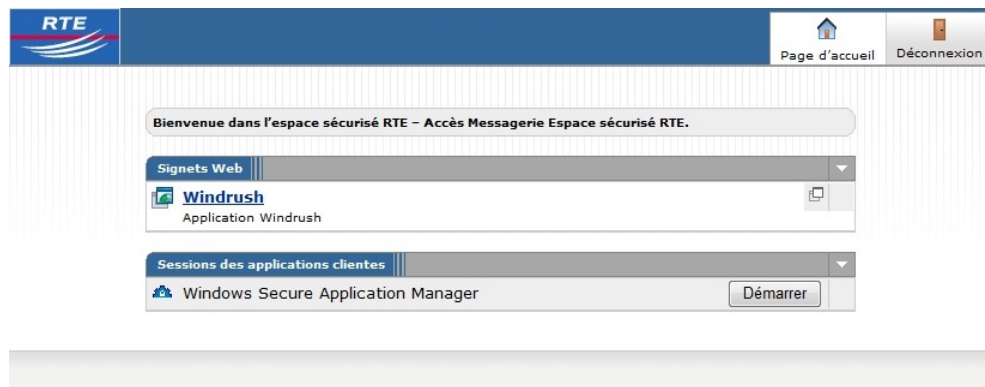


Please be patient through the entire installation procedure:



If your Internet access requires authentication with a proxy, a window will appear asking you for your connection identification credentials. Enter them and validate.

Once the installation has finished, the welcome page will be shown again:



Finally, the  icon will appear in your task bar.

Click on the **Disconnect** button (on the top right of the page) to terminate the session:



Bienvenue dans l'espace sécurisé RTE
Espace Sécurisé RTE

Votre session est terminée.

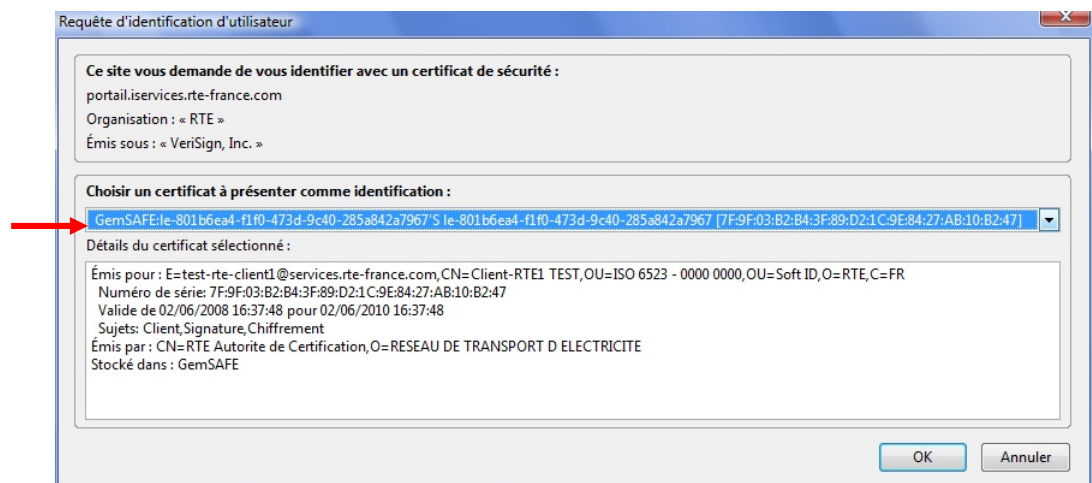
8.6.4 Use of the SSL VPN

8.6.4.1 Establishing the connection

Start your browser and enter the following URL:

<https://secure.iservices.rte-france.com>

This window will be displayed:

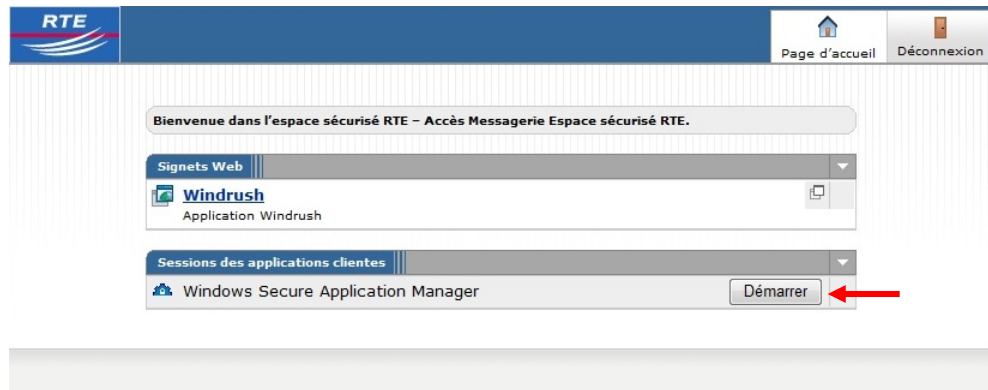


Select your certificate from the dropdown list labelled "Choose a certificate to present as identification" and click on "OK". If necessary, this window will ask you for the password to the Mozilla Firefox certificate store.



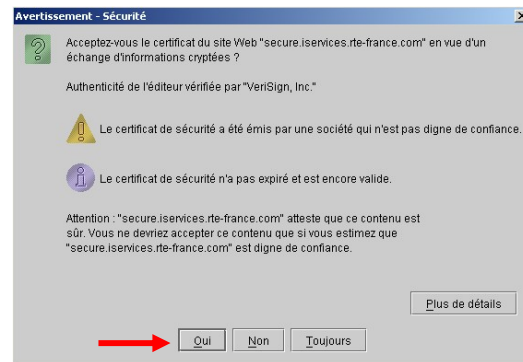
Then the following page will be displayed:

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



Click on the "Start" button to start the WSAM application.

If this window below appears, just click on **Yes**.



If your Internet access is protected by a proxy, a window will appear asking you for your connection identification credentials. Enter them and validate.

Finally, the  icon will appear in your task bar.

Notes:

- The certificate is only used to establish the SSL VPN connection.
- To close the SSL VPN session, click on the Disconnect button (on the top right of the page).

8.6.4.2 Using SSL VPN to access hosted email folders

SSL VPN can be used to access email folders hosted in FrontOffice with the use of a standard email client.

Access to the hosted email folders requires that the SSL VPN connection has been established (see §8.6.4.1).

The configuration of the email account in your email client software is made in the normal fashion with the following parameters:

- Email server type: POP server
- POP server address: **pop.services.rte-france.com**
- SMTP server address: **smtp.services.rte-france.com**

When your access to RTE FrontOffice is supplied to you, you will receive your login identifier, your password and your email address.



Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual

NOTE

Given that the messages are being forwarded through a secure channel,
**the sending and receipt of emails does not require the use of a
certificate for message encryption.**



E. EMAIL CLIENTS

9. Use of email clients

9.1 Certificates and email software

Depending on the email client that you use, we suggest that you refer to the appropriate one of the following sections.

Steps to follow:

- **install the "RTE Autorité de Certification" root certificate**, so that the email software trusts your certificates and the applications' certificates (refer to the installation of the RTE root certificate in the associated web browser),
- **configure your email account assigned for communications with RTE**, so that the email software always encrypts and signs your messages (being sent from the RTE IT system),
- **install the application certificate(s)**, so that messages that you send to those applications are encrypted.

Here are the associated web browsers that you should configure (if they have not already been done), in order that your email client is correctly configured and operational:

Email client	Associated web browser
Windows Mail	Internet Explorer
Outlook 2003	Internet Explorer
Outlook 2007	Internet Explorer
Mozilla Thunderbird	special configuration
Lotus Notes	configuration is specific to Lotus Notes

9.2 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications,
- sign and encrypt emails destined for RTE applications,
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add to contacts" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Outlook 2000 does.

Important note

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

10. Windows Mail

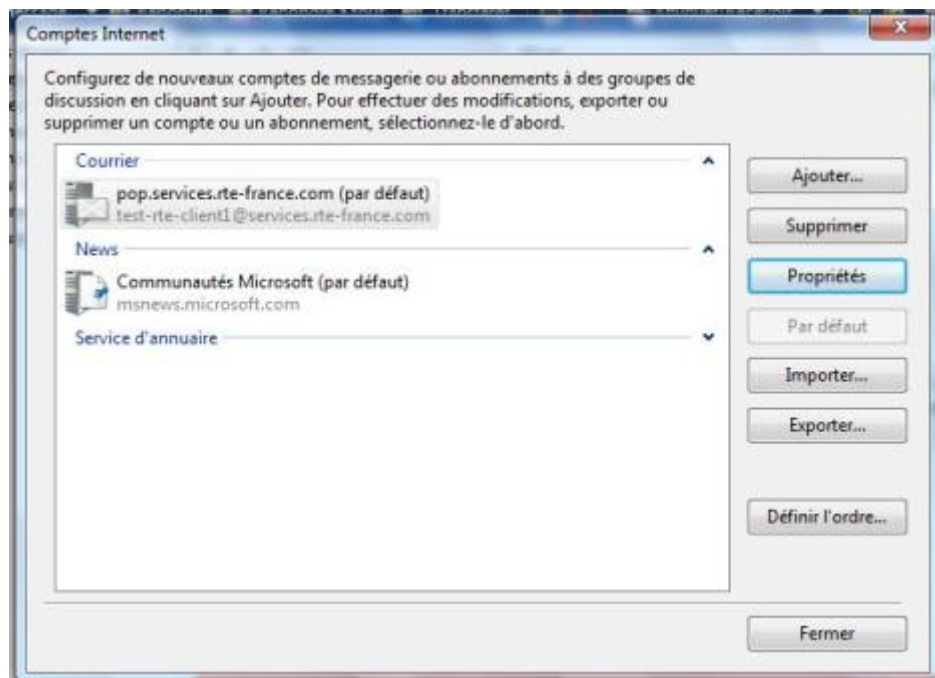


10.1 Preliminary configuration

To associate your certificate with your email account under Windows Mail, your certificate must be installed under Internet Explorer. This is automatically the case if you have downloaded it in Internet Explorer; but if you downloaded it with Mozilla Firefox, you must export it from that browser and import it into Internet Explorer, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

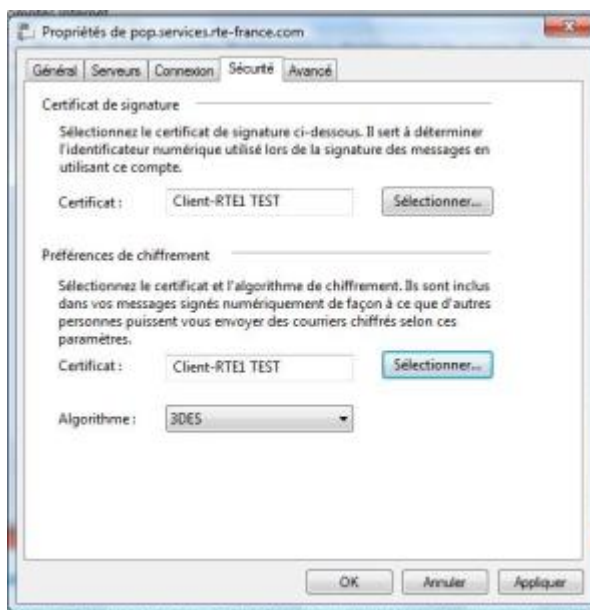
Windows Mail automatically associates an account with the certificate carrying the same email address in order to sign messages.

To configure Windows Mail, start the "Tools > Accounts..." menu option and select the "Email" tab:



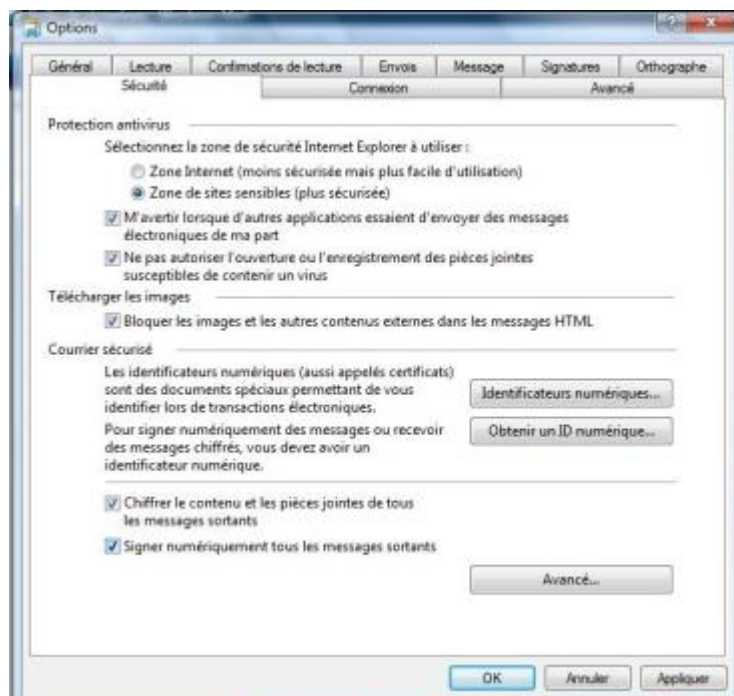
Select your RTE communications account and click on "Properties":

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual

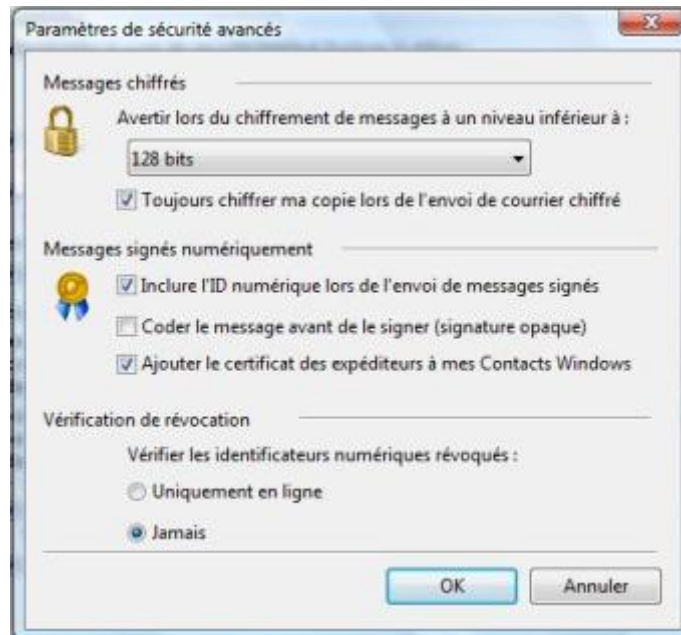


Then click on the **"Security"** tab, and use the two **"Select..."** buttons to select your certificate for signing and encryption. Select the **3DES** algorithm. Then click on **"OK"**.

Still from within Windows Mail, start the **"Tools > Options..."** menu:



Select the **"Security"** tab, check the two checkboxes labelled **"Encrypt the contents of messages and attached documents for outgoing messages"** and **"Digitally sign all outgoing messages"**, and then click on the **"Advanced"** button:



Verify that the configuration is identical to that above; please specifically check the two boxes labelled "Include the digital identification when sending messages" and "Add the certificate of senders to the address book" have been checked; then click on "OK".

All your emails destined for RTE applications sent from this account will now be encrypted and signed.

10.2 Use of the certificate

10.2.1 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications;
- sign and encrypt emails destined for RTE applications;
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add to the address book" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

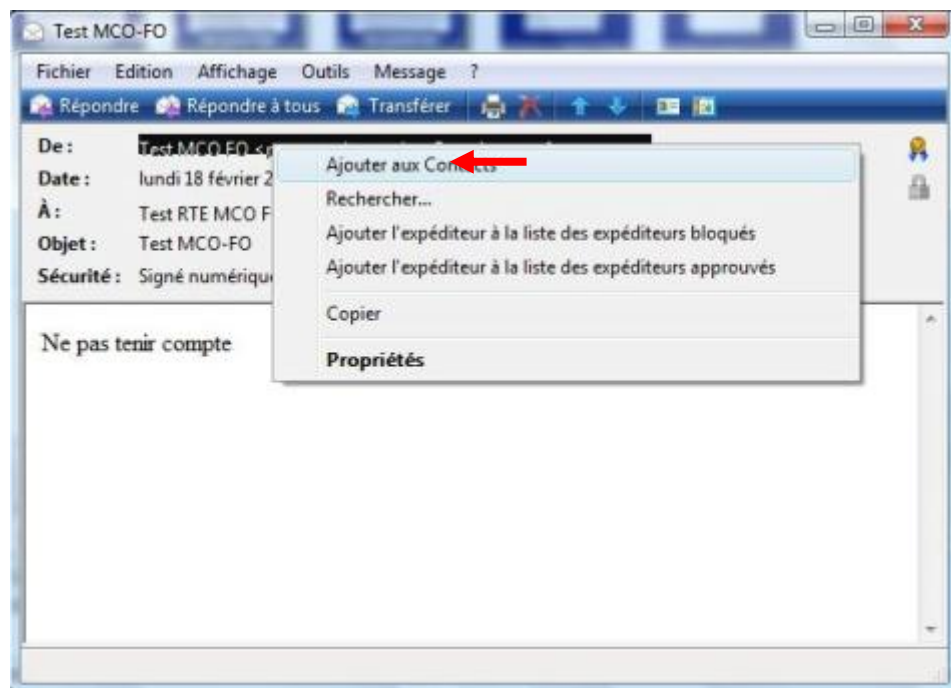
The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Windows Mail does.

IMPORTANT NOTE

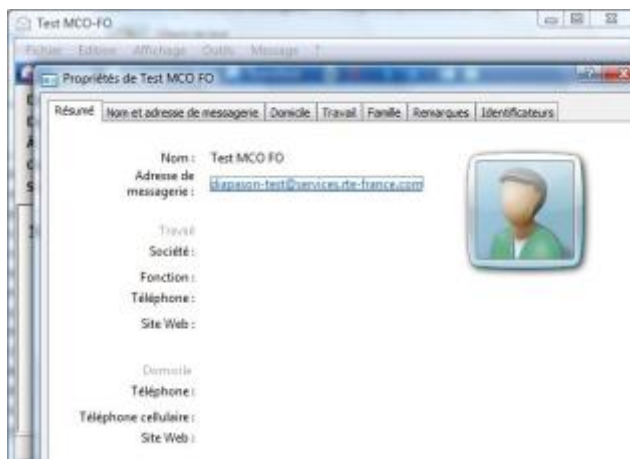
The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

10.2.2 Application certificates

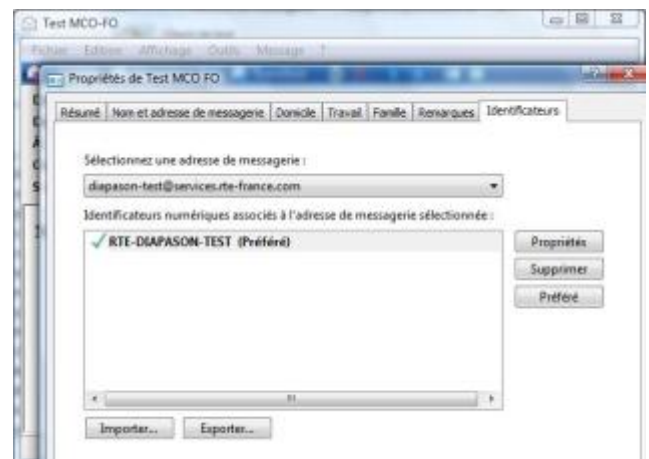
Upon receiving the first signed and encrypted message from an application, you should install the sending application's certificate. To do so, you must add the application's email address to your address book by clicking on **"Add to the address book"** with the right mouse button when positioned over the sender's name of the message received:



The "Summary" tab:



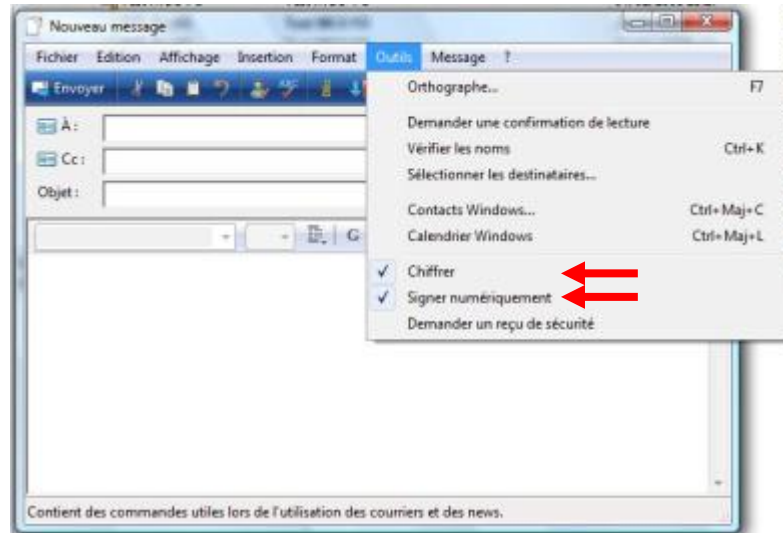
The "Identifiers" tab:



Click on the "OK" button to validate.

10.2.3 Message encryption and signing

To encrypt and sign a message with Windows Mail, first create a new message by clicking on "Create a message" (or Ctrl+N),



Verify that the two boxes "**Encrypt**" and "**Sign digitally**" have been checked.

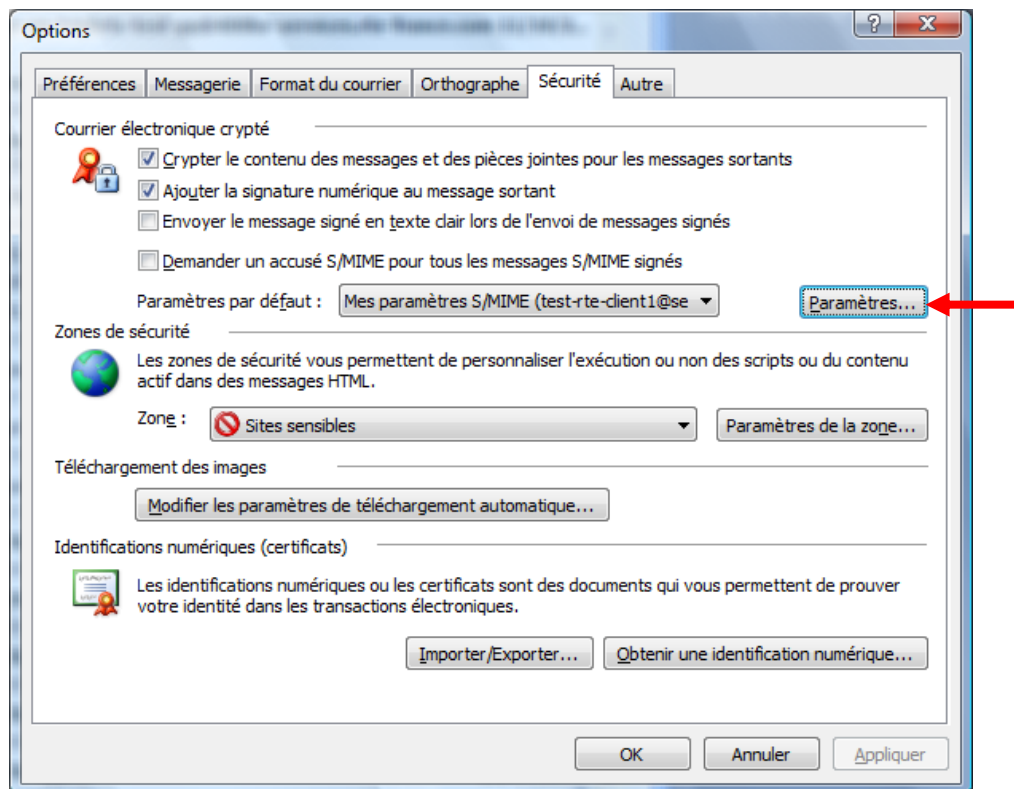
11. Outlook 2003



11.1 Preliminary configuration

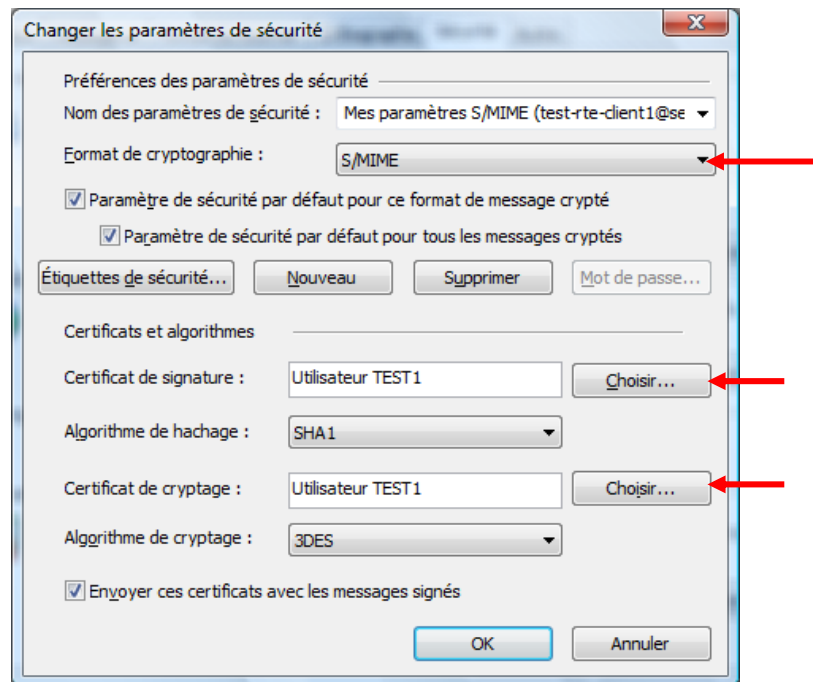
To be able to associate your certificate with your email account under Outlook 2003, your certificate must be installed under Internet Explorer. This is automatically the case if you have downloaded it in Internet Explorer; but if you downloaded it with Mozilla Firefox, you must export it from that browser and import it into Internet Explorer, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

Start Outlook 2003 and open the menu option "Tools > Options...":

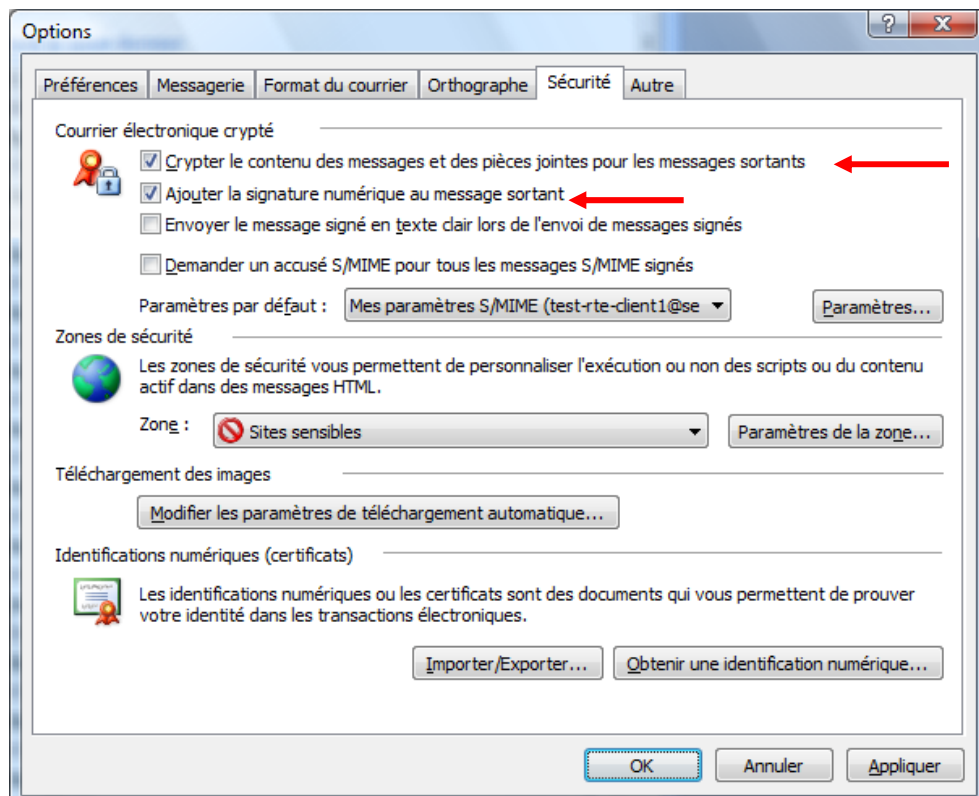


Select the "Security" tab, then click on the "Parameters..." button:

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



Click on the two "Select..." buttons in order to select your certificate for signing and encryption from the list of selectable certificates that is presented to you (you can also display any certificate in the list to view its contents and assure yourself that you have chosen the right one). Finally, verify that the data is the same as that above (S/MIME, boxes checked, certificates, algorithms); if the "Name of the security parameters" field is empty, enter a name like "RTE Certification". At last, click on "OK". The following window will then be displayed:



Check the "Encrypt the contents of messages and attached documents for outgoing messages" and "Add the digital signature to outgoing messages" boxes and click on "OK".

All your emails destined for RTE applications sent from the default account will now be encrypted and signed.

11.2 Use of the certificate

11.2.1 When to use the certificate

By using your certificate, you can:

authenticate yourself to RTE applications;

sign and encrypt emails destined for RTE applications;

decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add to contacts" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Outlook 2003 does.

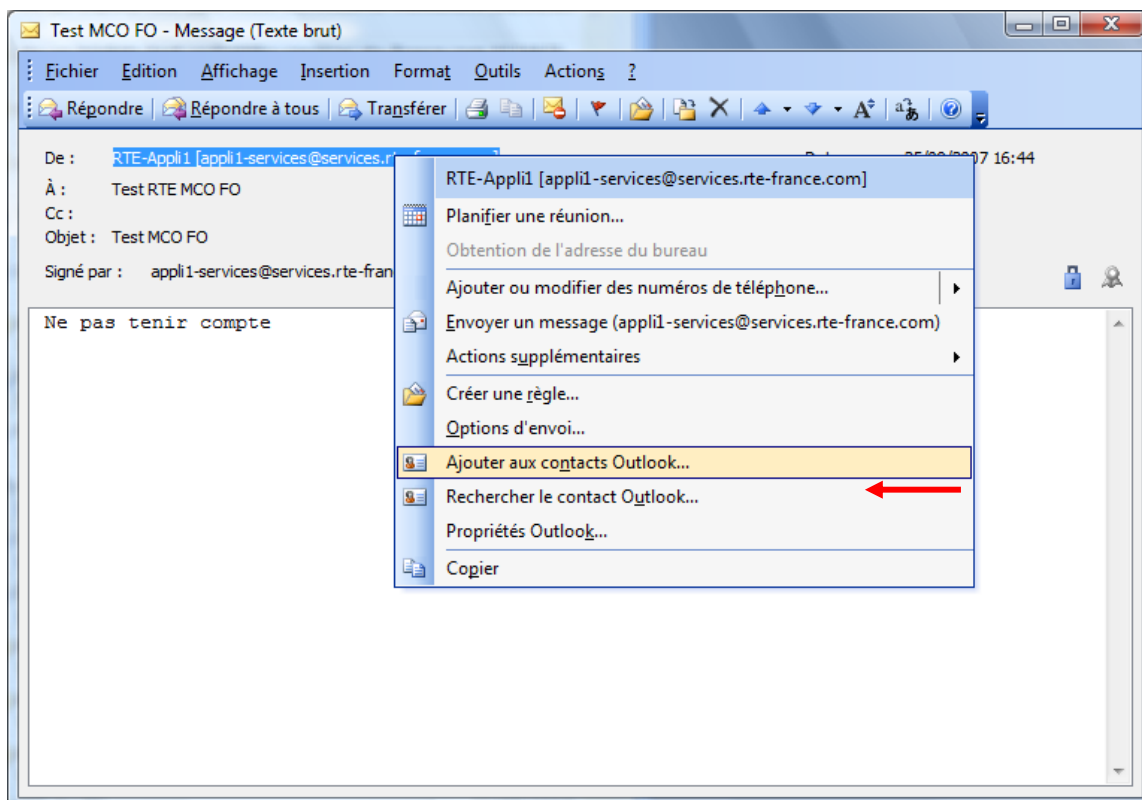
IMPORTANT NOTE

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

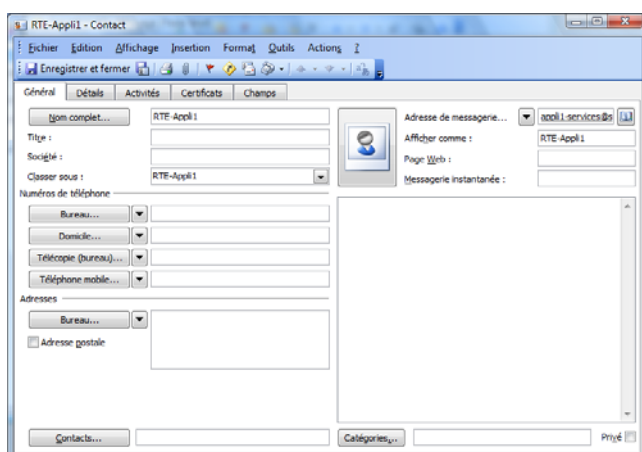
11.2.2 Application certificates

Upon receiving the first signed and encrypted message from an application, you should install the sending application's certificate. To do so, you must add the application's email address to your address book by clicking on "**Add to contacts**" with the right mouse button when positioned over the sender's name of the message received:

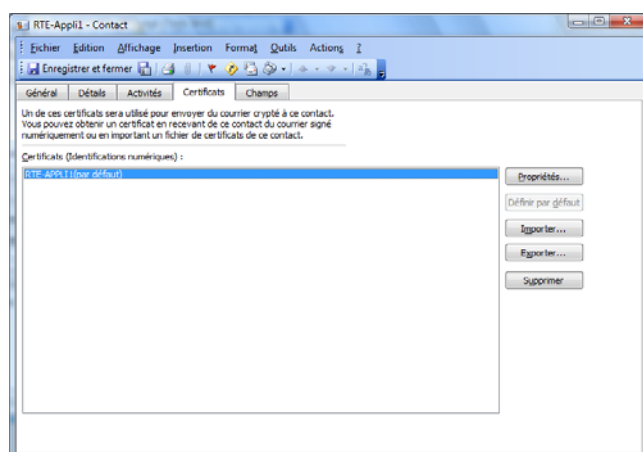
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



The "General" tab:



The "Certificates" tab:

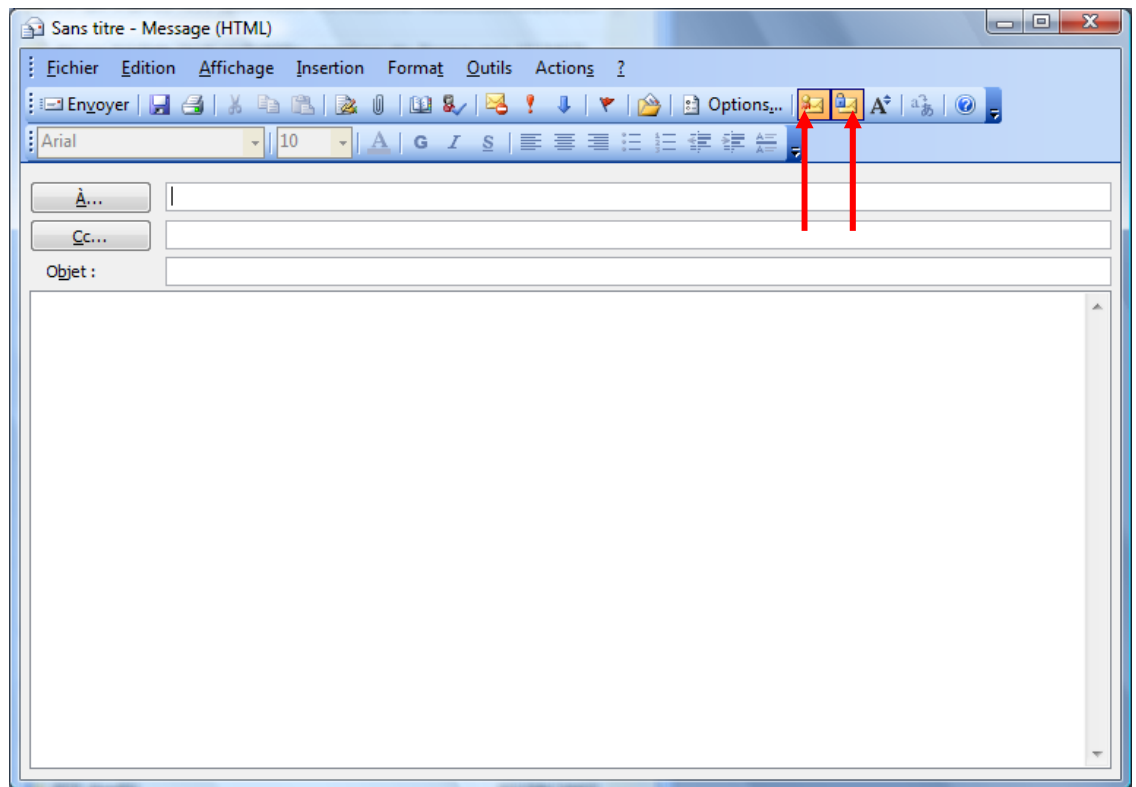


"Ctrl+S" to save.

11.2.3 Message encryption and signing

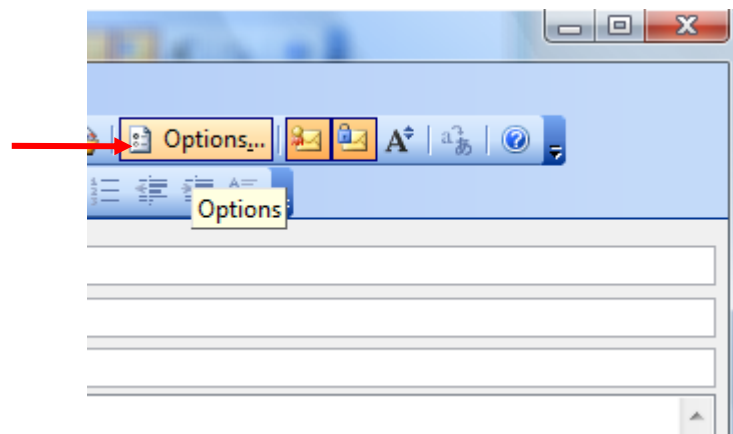
To encrypt and sign a message with Outlook 2003, first create a new message by clicking on "New" (or Ctrl+N),

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual

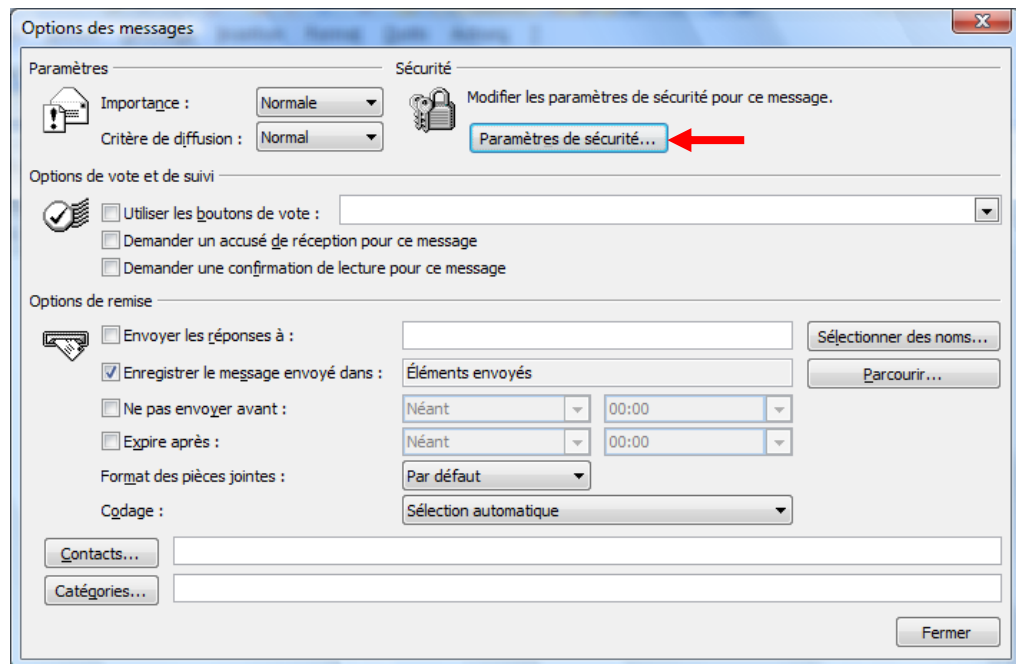


To sign and encrypt your message, verify that the two icons above have been correctly checked.

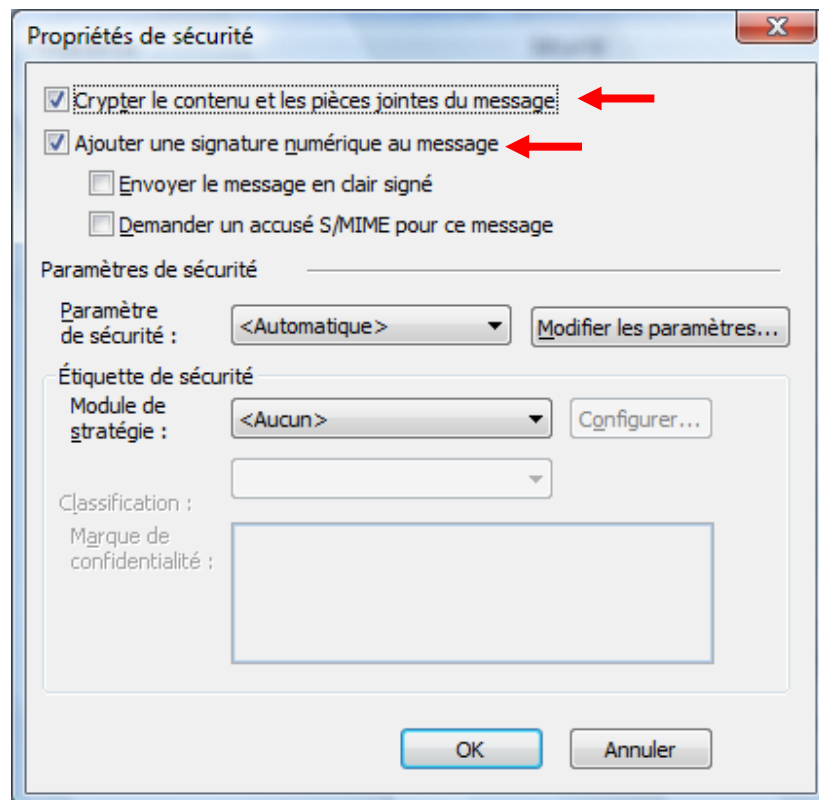
To verify the security parameters, right click on the "**Options...**" button.



Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



Click on the "**Security parameters...**" button.



Verify that the boxes labelled "**Encrypt the message content and attached documents**" and "**Add a digital signature to the message**" have been checked by default.

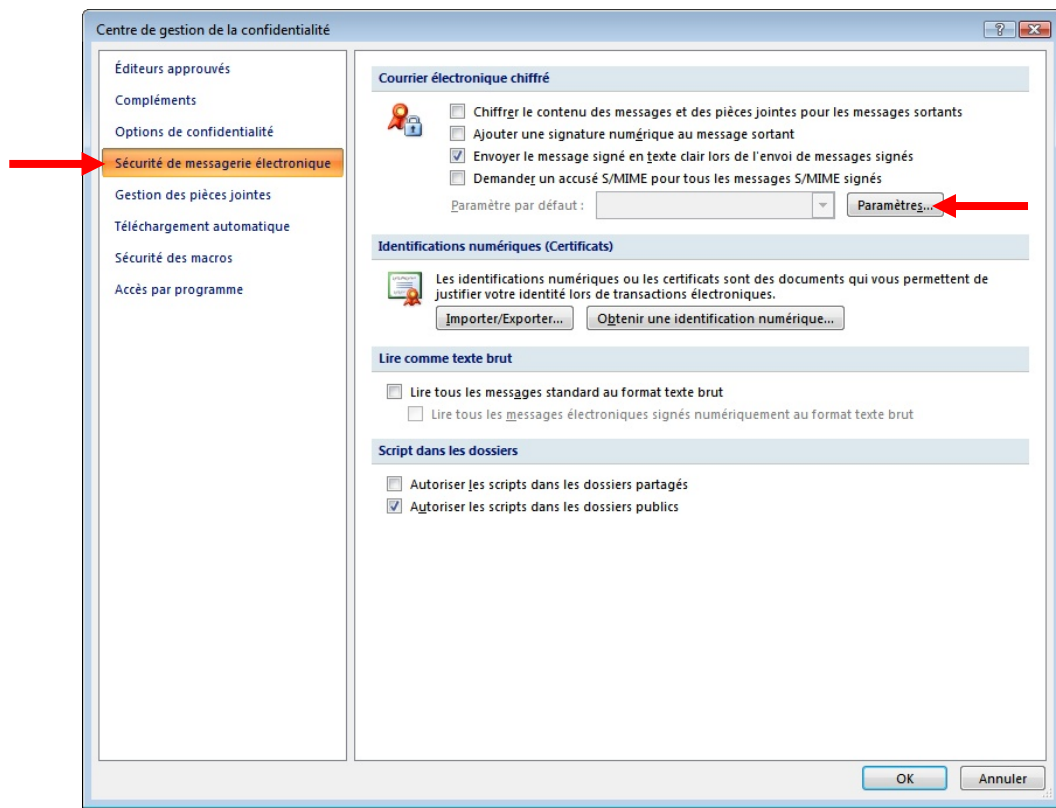
12. Outlook 2007



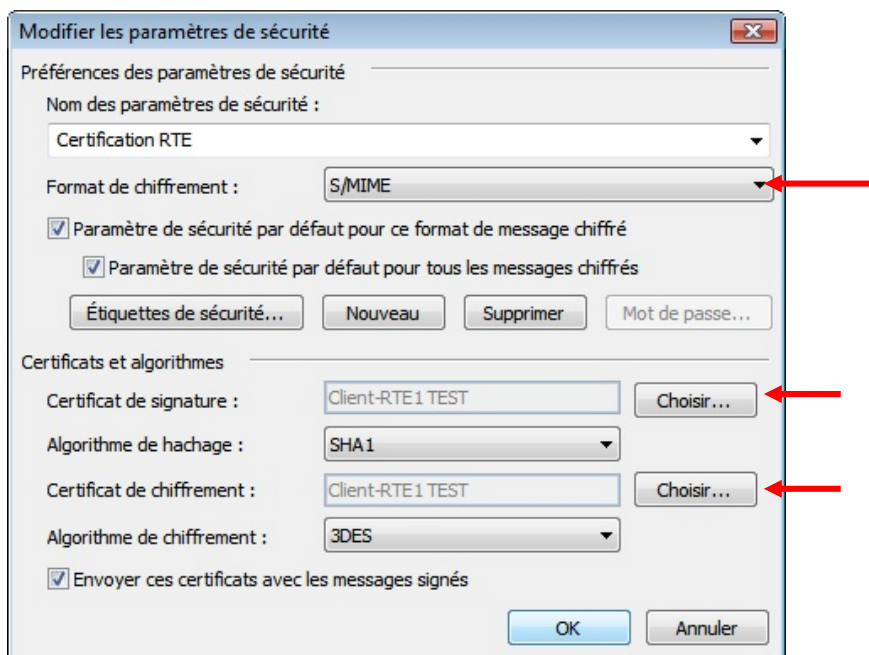
12.1 Preliminary configuration

To be able to associate your certificate with your email account under Outlook 2007, your certificate must be installed under Internet Explorer. This is automatically the case if you have downloaded it in Internet Explorer; but if you downloaded it with Mozilla Firefox, you must export it from that browser and import it into Internet Explorer, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

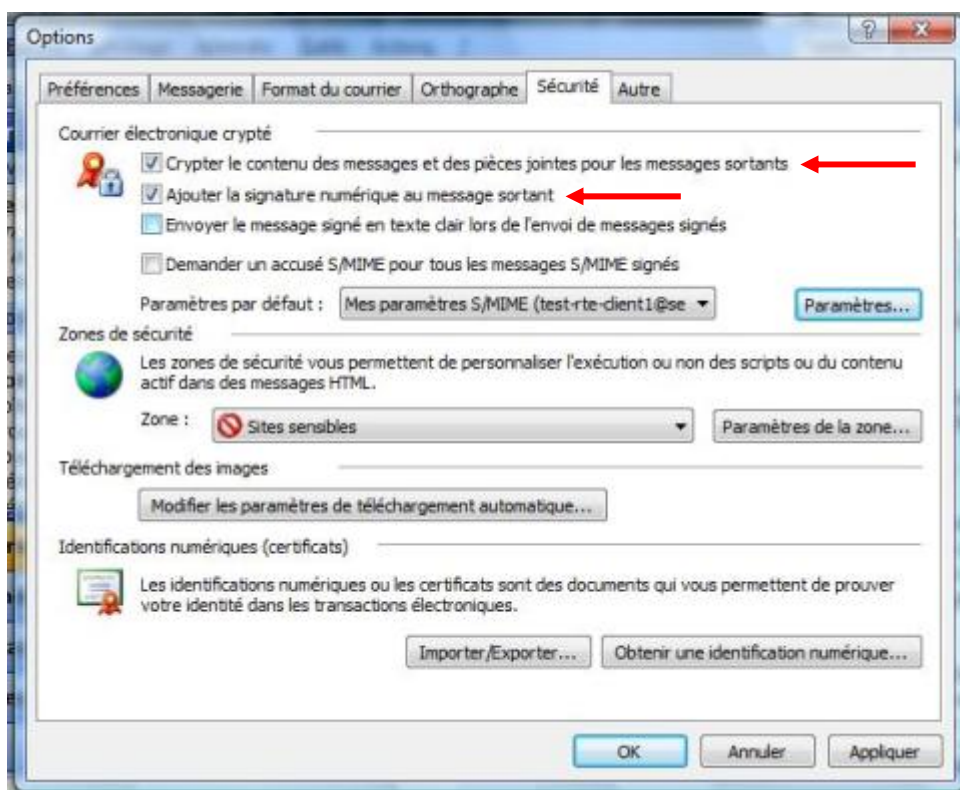
Start Outlook 2007 and open the menu option "Tools > Confidentiality management centre...".



In the right hand column, click on "Email security" and then click on the "Parameters..." button.



Click on the two "Select..." buttons in order to select your certificate for signing and encryption from the list of selectable certificates that is presented to you (you can also display any certificate in the list to view its contents and assure yourself that you have chosen the right one). Finally, verify that the data is the same as that above (S/MIME, boxes checked, certificates, algorithms); if the "Name of the security parameters" field is empty, enter a name like "RTE Certification". At last, click on "OK". The following window will then be displayed:



Check the "Encrypt the contents of messages and attached documents for outgoing messages" and "Add a digital signature to outgoing messages" boxes and click on "OK".

All your emails destined for RTE applications sent from the default account will now be encrypted and signed.

12.2 Use of the certificate

12.2.1 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications;
- sign and encrypt emails destined for RTE applications;
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add to contacts" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Outlook 2007 does.

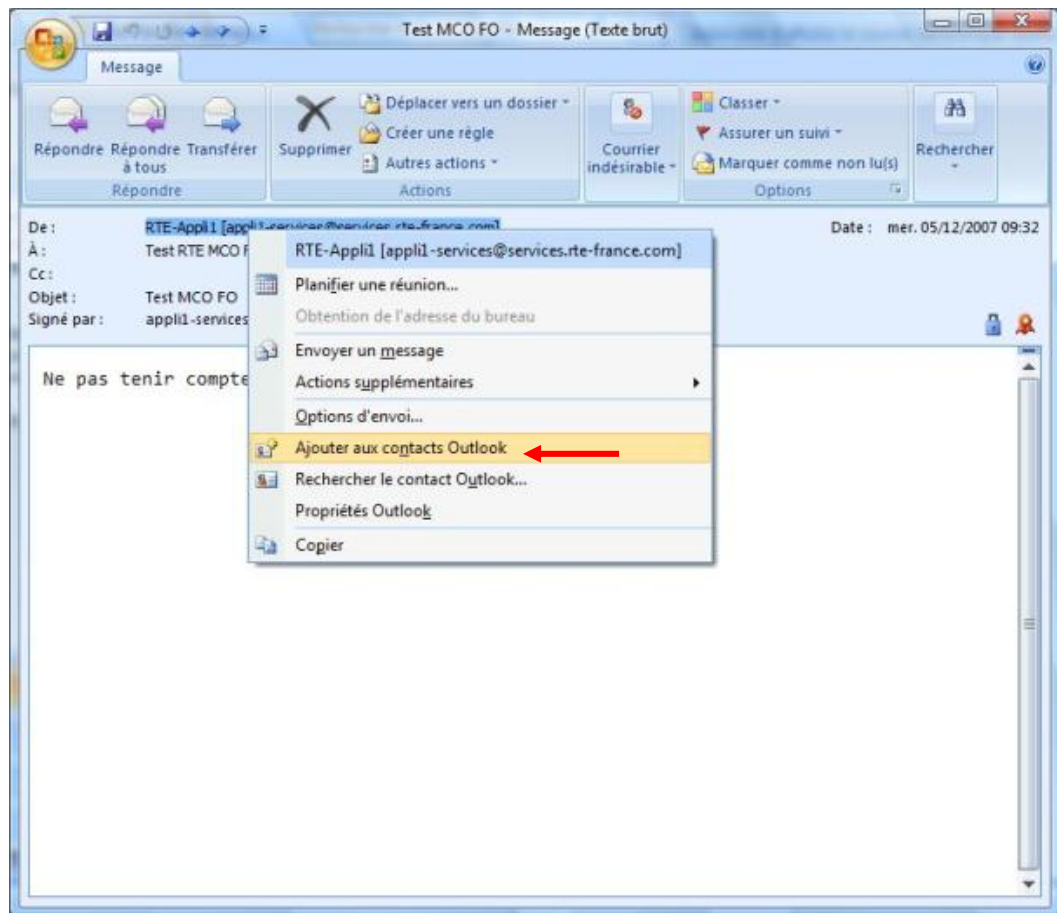
IMPORTANT NOTE

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

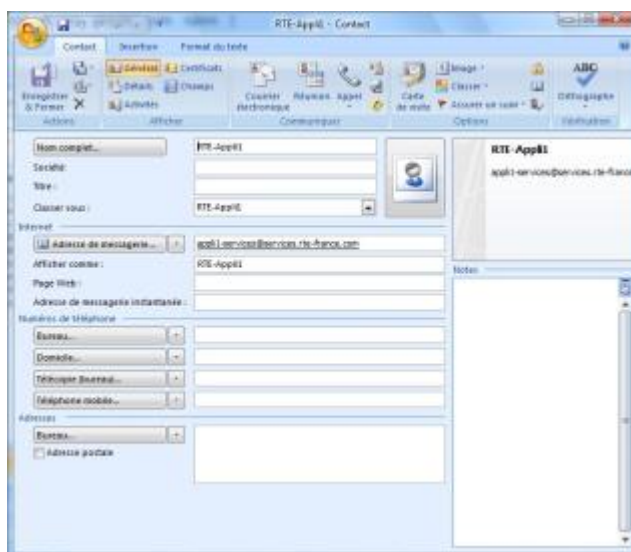
12.2.2 Application certificates

Upon receiving the first signed and encrypted message from an application, you should install the sending application's certificate. To do so, you must add the application's email address to your address book by clicking on "**Add to contacts**" with the right mouse button when positioned over the sender's name of the message received:

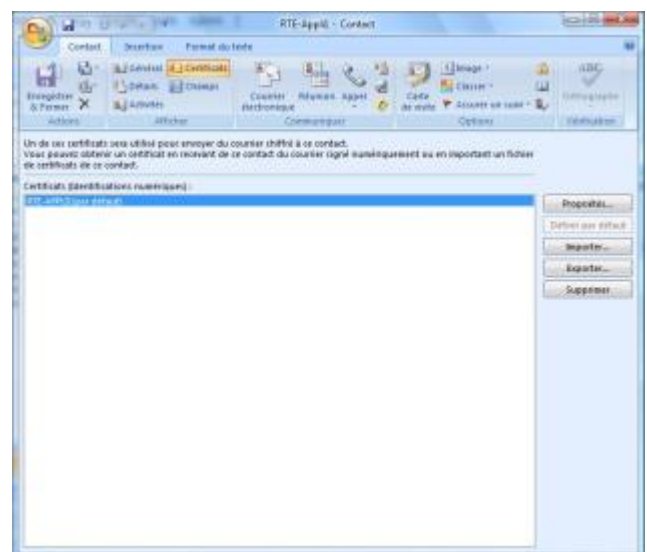
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



The "General" tab:



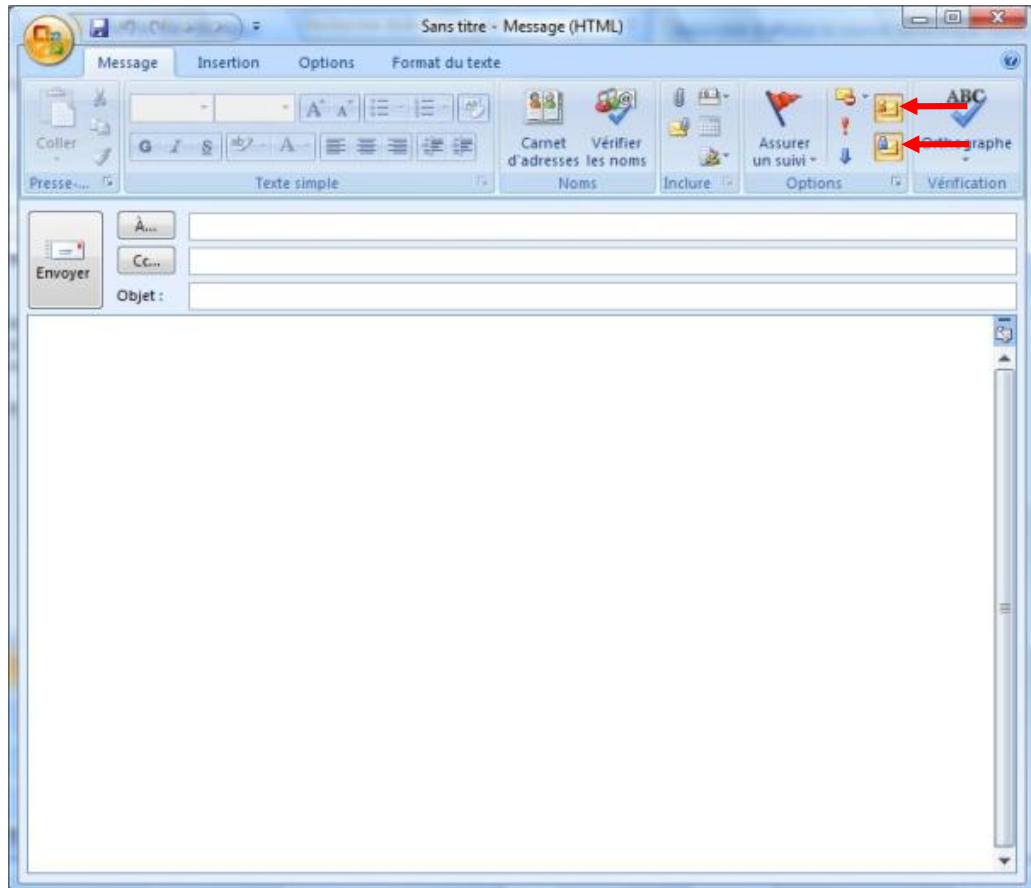
The "Certificates" tab:



"Ctrl+S" to save.

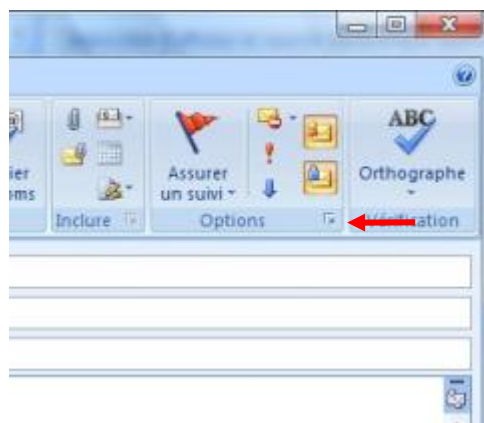
12.2.3 Message encryption and signing

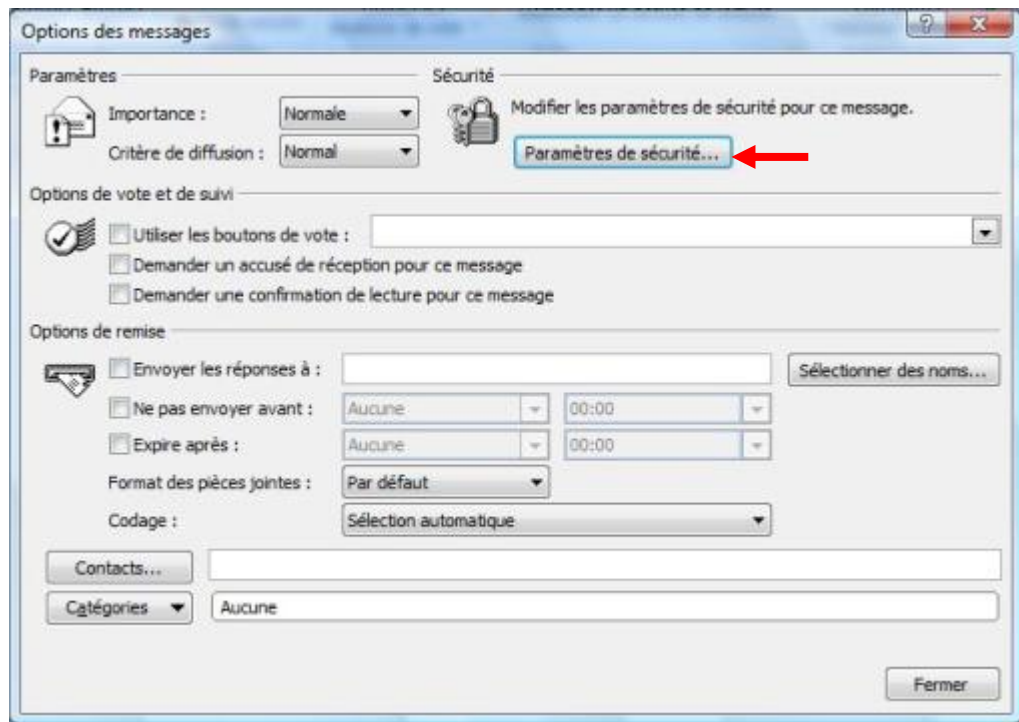
To encrypt and sign a message with Outlook 2007, first create a new message by clicking on "New" (or Ctrl+N),



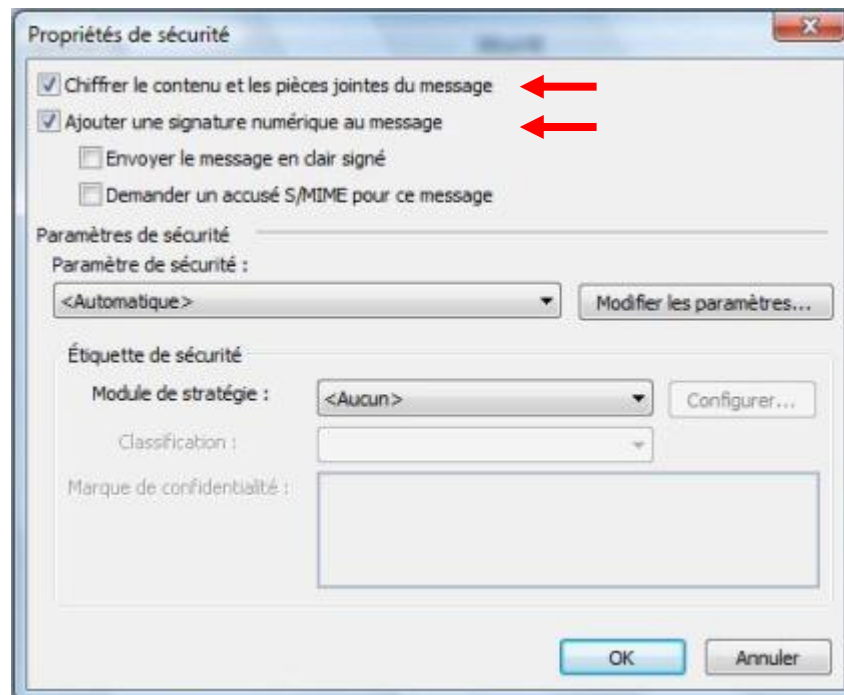
To sign and encrypt your message, verify that the two icons above have been correctly checked.

To verify the security parameters, right click on the "**Options...**" button.





Click on the "**Security parameters...**" button.



Verify that the boxes labelled "**Encrypt the message content and attached documents**" and "**Add a digital signature to the message**" have been checked by default.

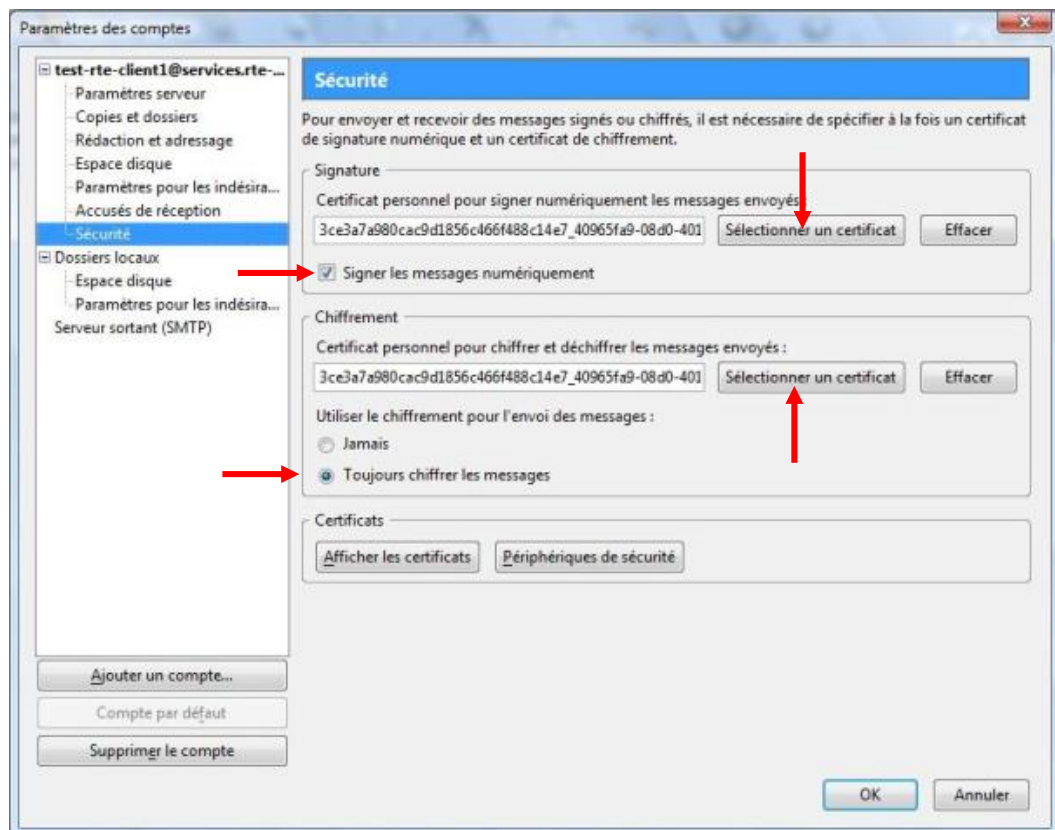
13. Mozilla Thunderbird



13.1 Preliminary configuration

To be able to associate your certificate with your email account under Mozilla Thunderbird, your certificate must be installed under Mozilla Thunderbird. To do this, you must export it from the browser that you installed it into, and import it into Mozilla Thunderbird, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

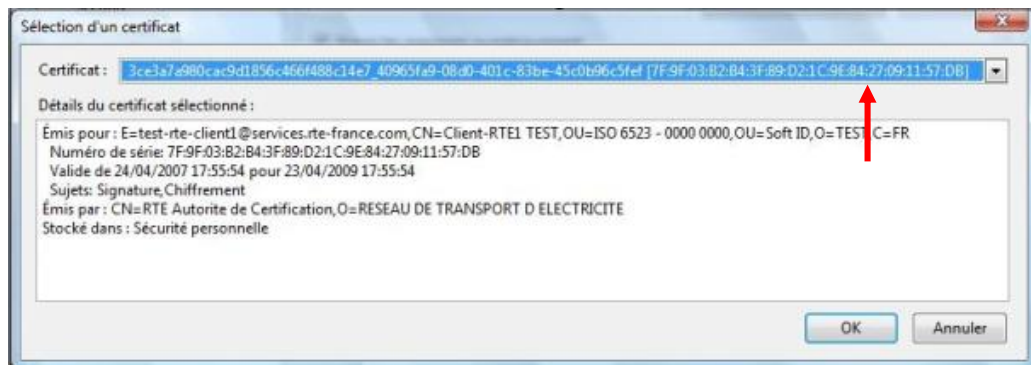
Start Mozilla Thunderbird, and open the "**Tools > Account parameters...**" menu, then select the "**Security**" item of the RTE communications accounts (e.g. "Client RTE 1"):



Click on "**Select a certificate**" to select (see above) your certificate for signing and encryption.

NOTE

Regarding the phrase "**for encryption**": the text indicates that your certificate will be used for "encrypting and decrypting messages sent", even though in reality it will only be used to decrypt messages received.



All your emails destined for RTE applications sent from this account will now be encrypted and signed.

13.2 Use of the certificate

13.2.1 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications;
- sign and encrypt emails destined for RTE applications;
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add the address to the address book" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Mozilla Mail does.

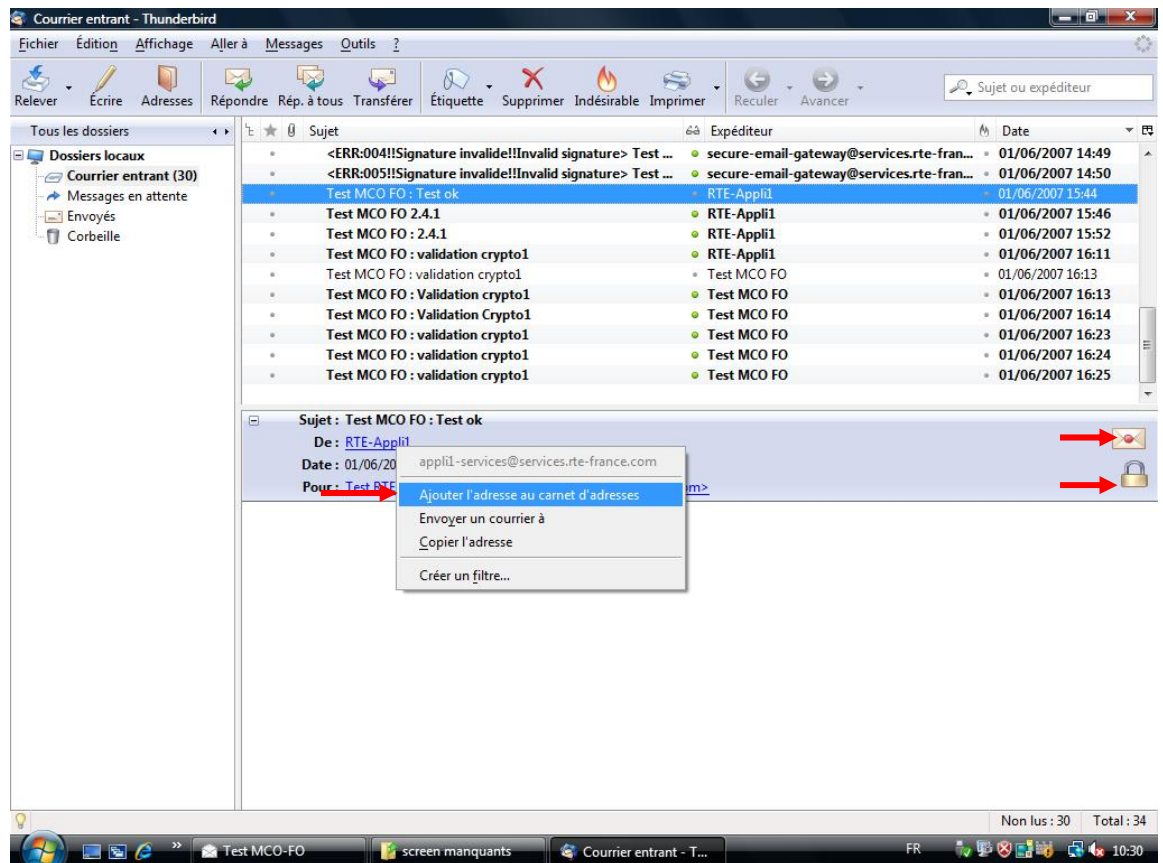
IMPORTANT NOTE

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

13.2.2 Application certificates

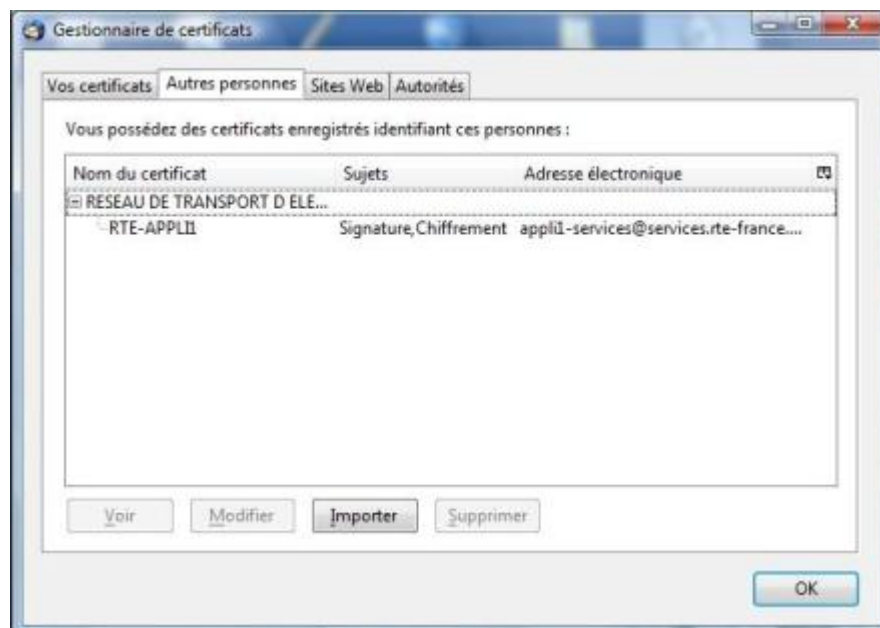
The installation of an application certificate is done automatically when the first email signed and encrypted sent by that application is read. Nevertheless, you

can add the application's email address to your address book by clicking on **"Add this address to the address book"**.



Whenever you see the window "New file for [RTE - DIAPASON]" appearing, just click on "OK".

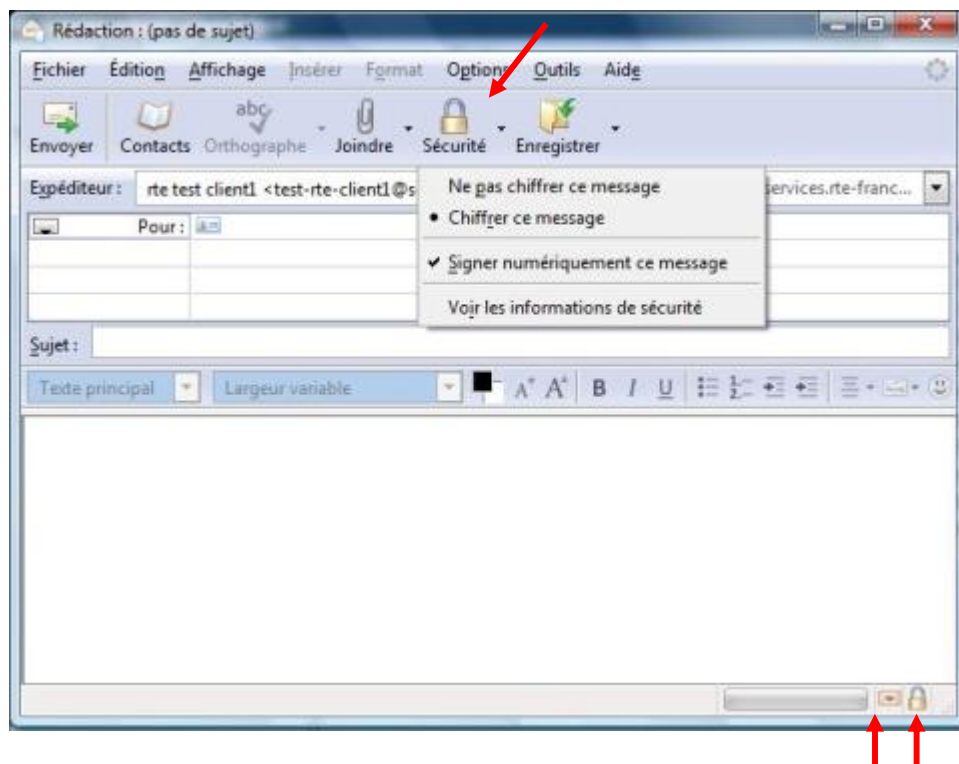
To verify that the application certificate (e.g. "RTE - DIAPASON") is correctly installed, open the "Tools > Options..." menu, select the "Confidentiality" section and the "Security" tab, then click on "View the certificates" and finally click on the "Other people" tab.



13.2.3 Message encryption and signing

To encrypt and sign a message with Mozilla Thunderbird, first create a new message by clicking on "Write" (or Ctrl+M),

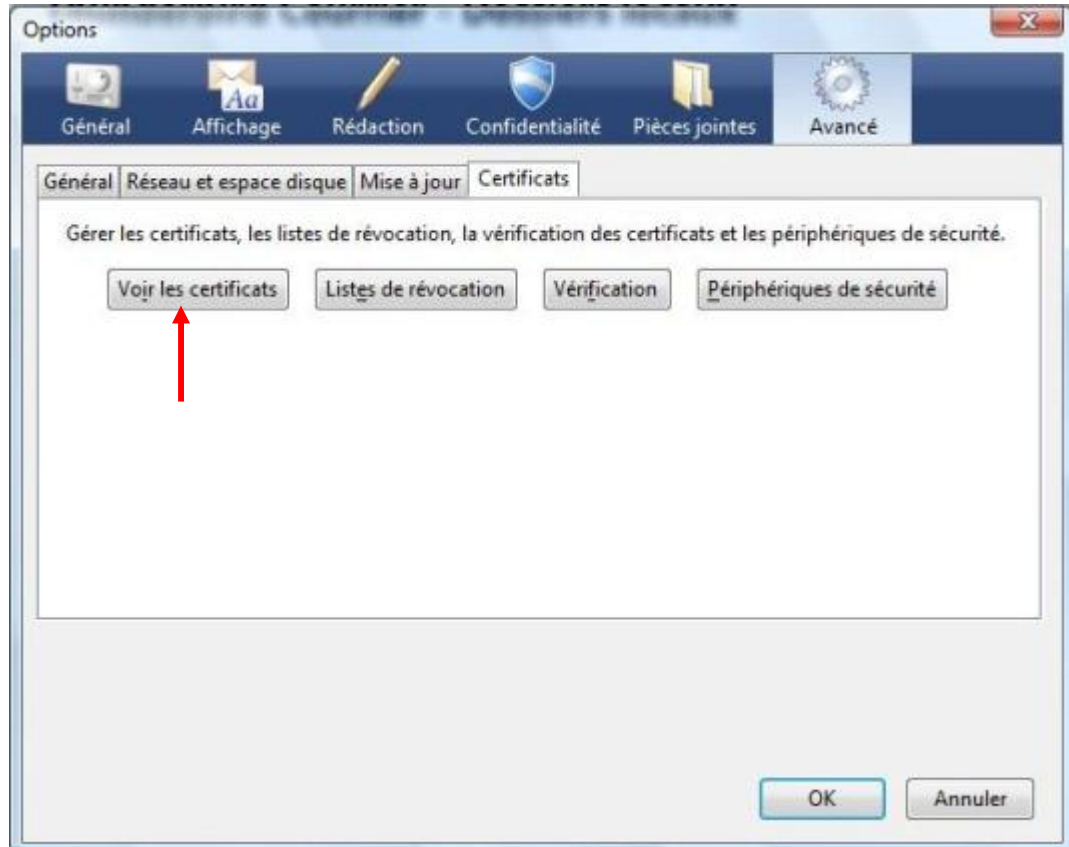
Click on the "Security" button to make sure the two options "**Encrypt this message**" and "**Digitally sign this message**" have been selected (these options ought to be selected by default).



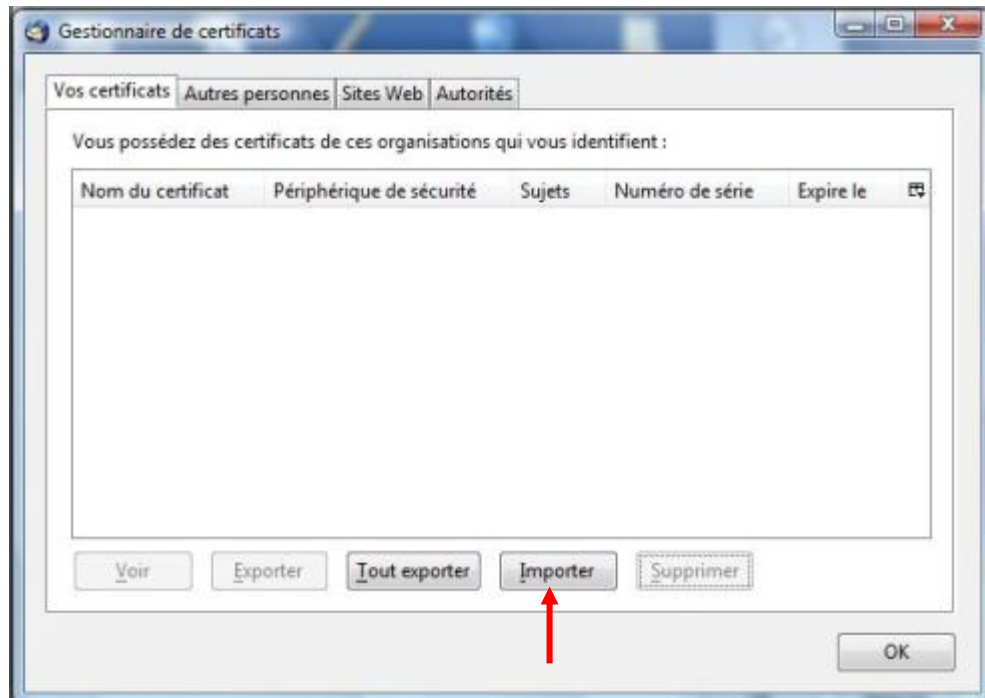
13.3 Importing the certificate

With Mozilla Thunderbird (v. 1.5), import of a complete PKCS#12 file with the root certificate.

Open the "Tools > Options..." menu, the "Confidentiality" section and then the "Security" tab (v. 1.5 and higher):

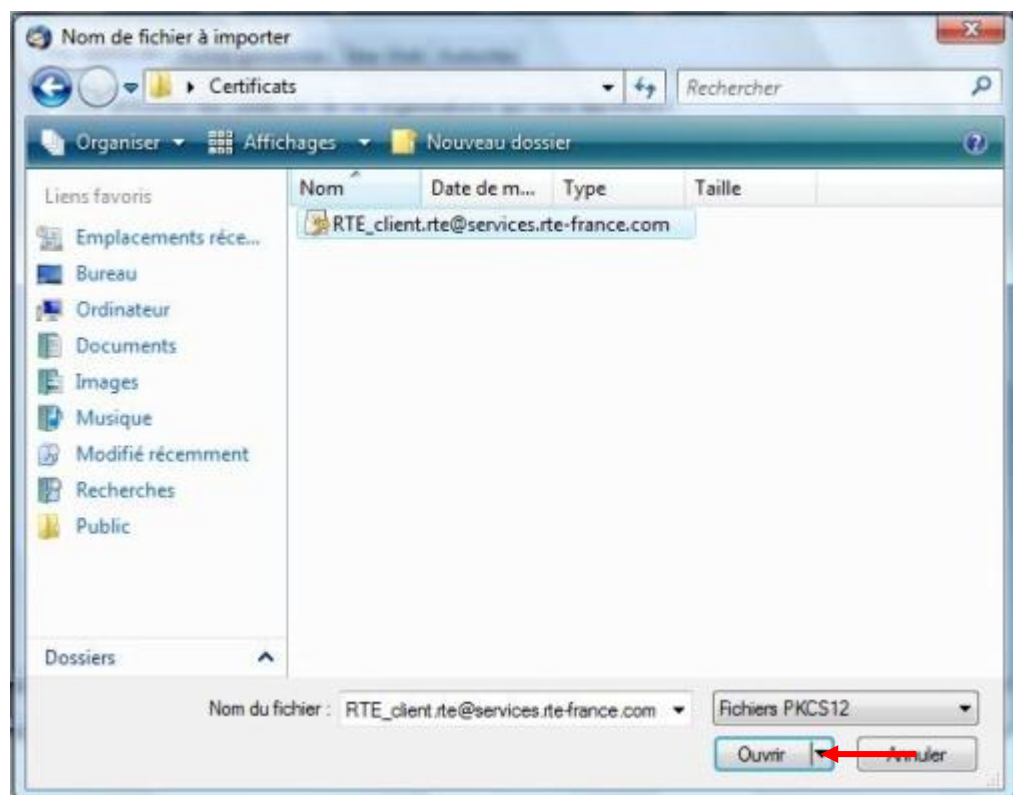


Click on the "View the certificates" button.



Click on the "Import" button:

Select the PKCS#12 file (with a ".p12" or ".pfx" extension):



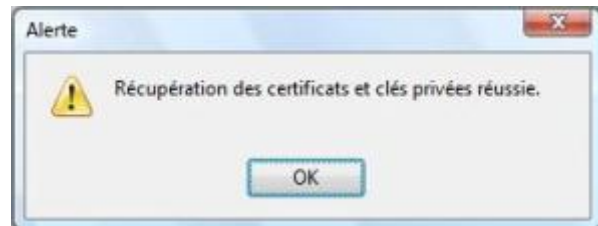
Enter the protection password
for the certificate store.

Enter the password restricting
access to the PKCS#12
(.p12) file, then click on "OK".

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual

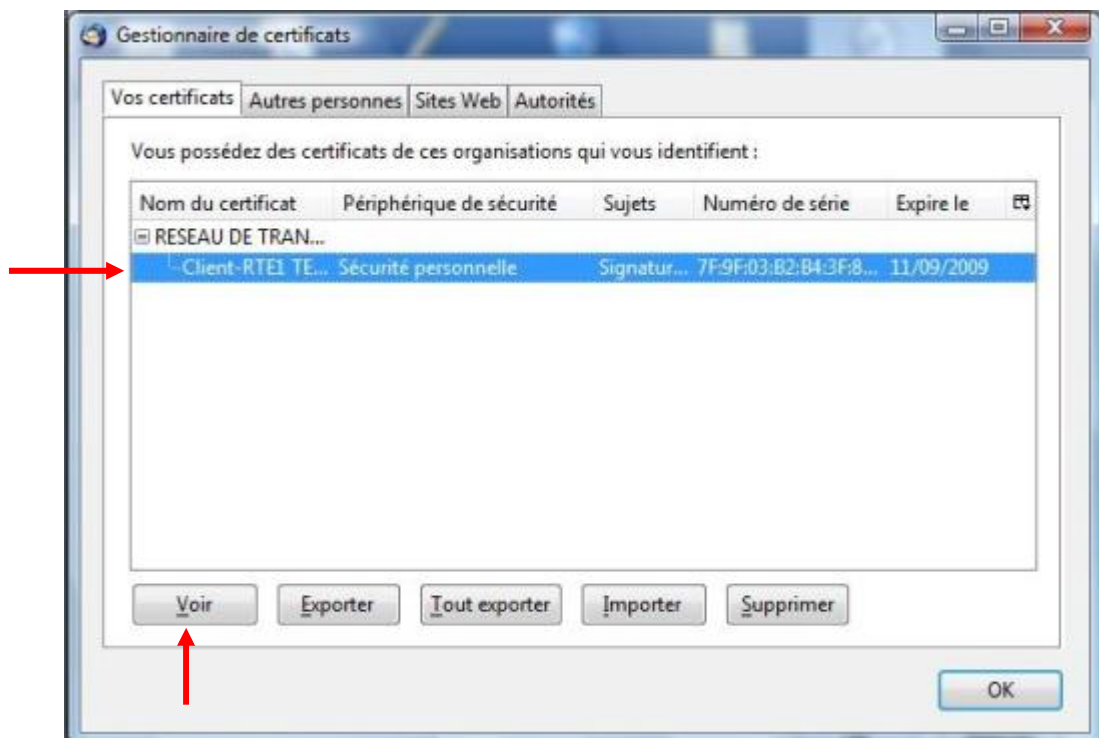


Click on "OK".



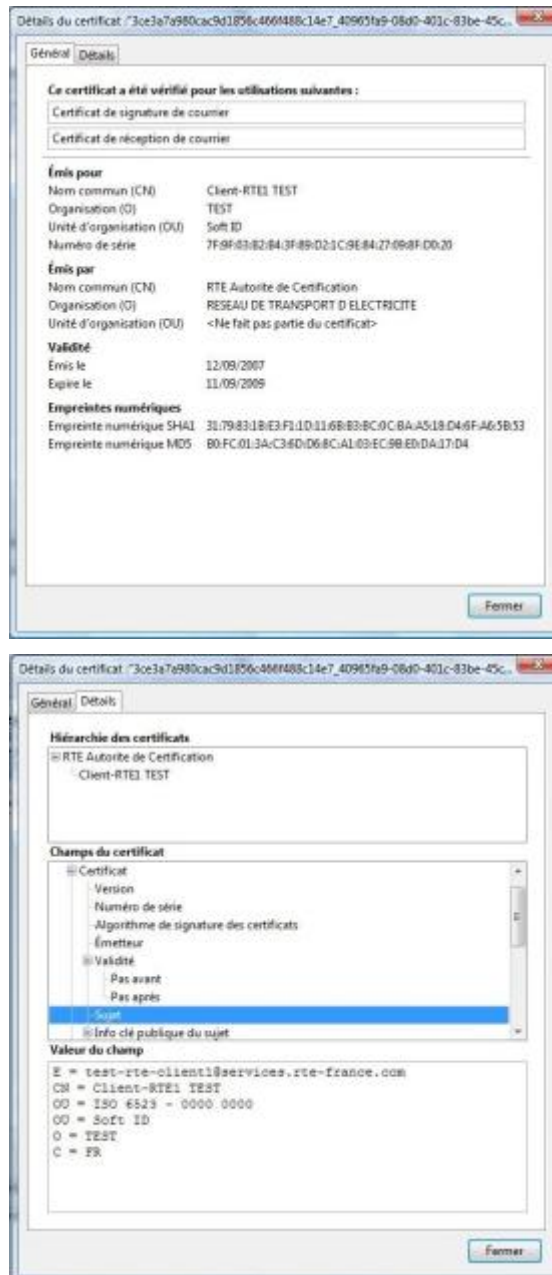
Note: if this password already exists, a field entry form will appear.

Your certificate is now in the Mozilla Thunderbird certificate store:

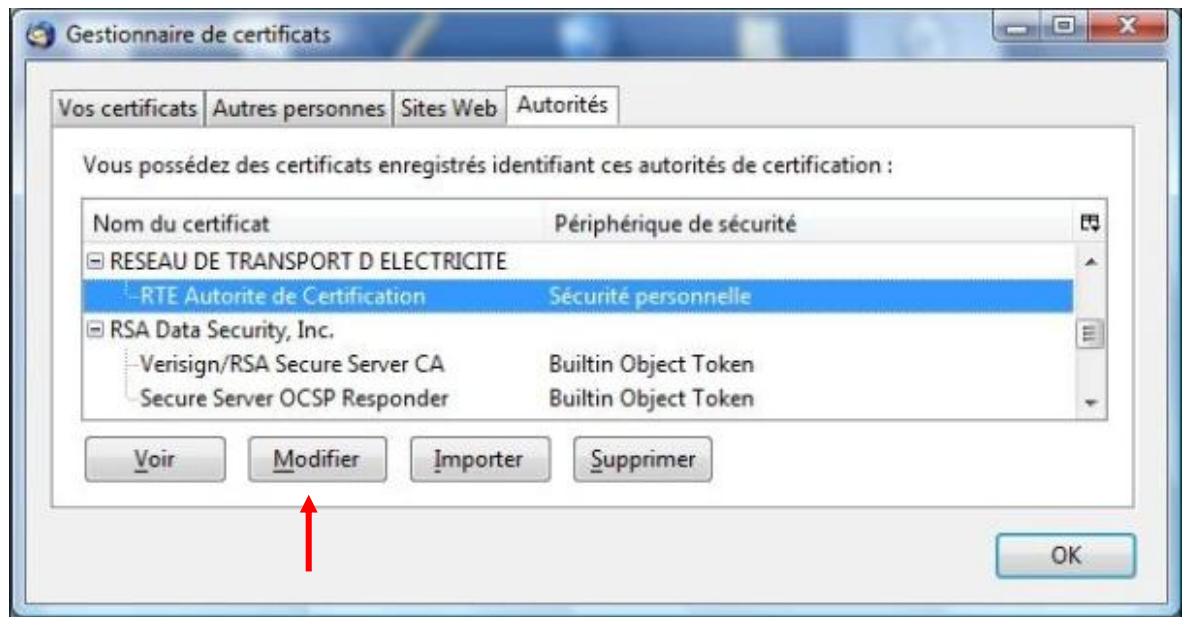


Check that it's the right one by clicking on the "View" button.

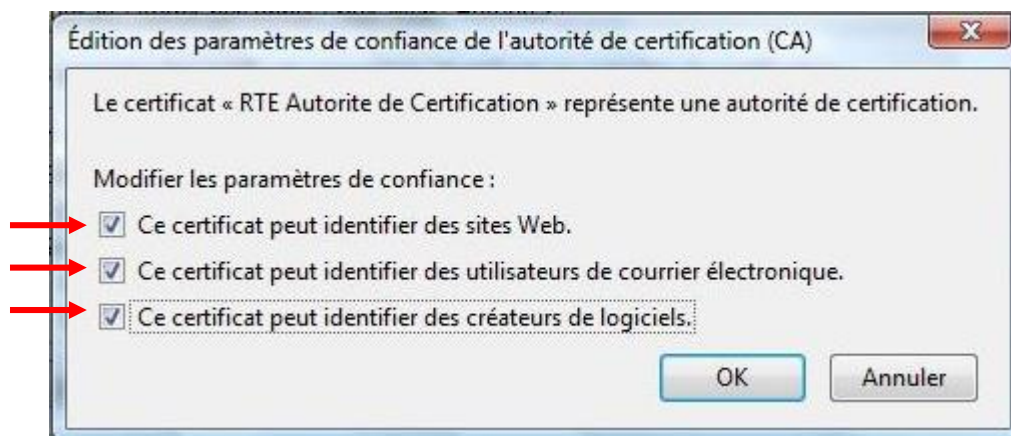
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



The RTE CA certificate is also in the Mozilla Thunderbird store:

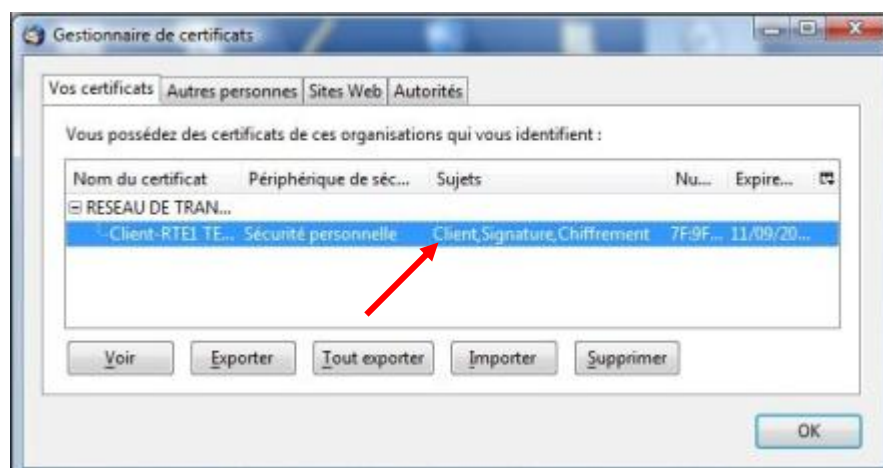


Click on the "Modify" button.

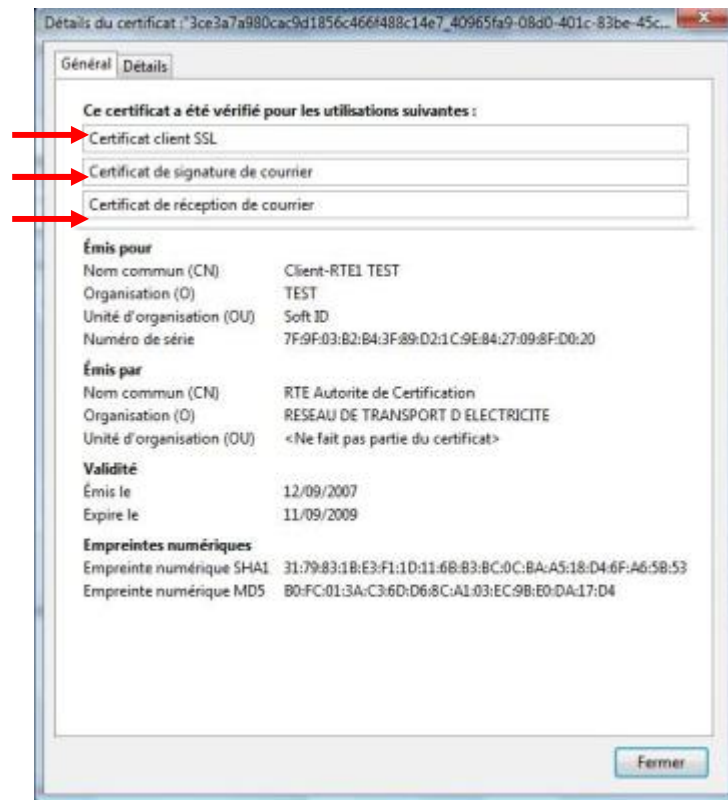


Check the three boxes shown above, then click on "OK".

You have now declared your trust in the RTE root certificate as shown below:



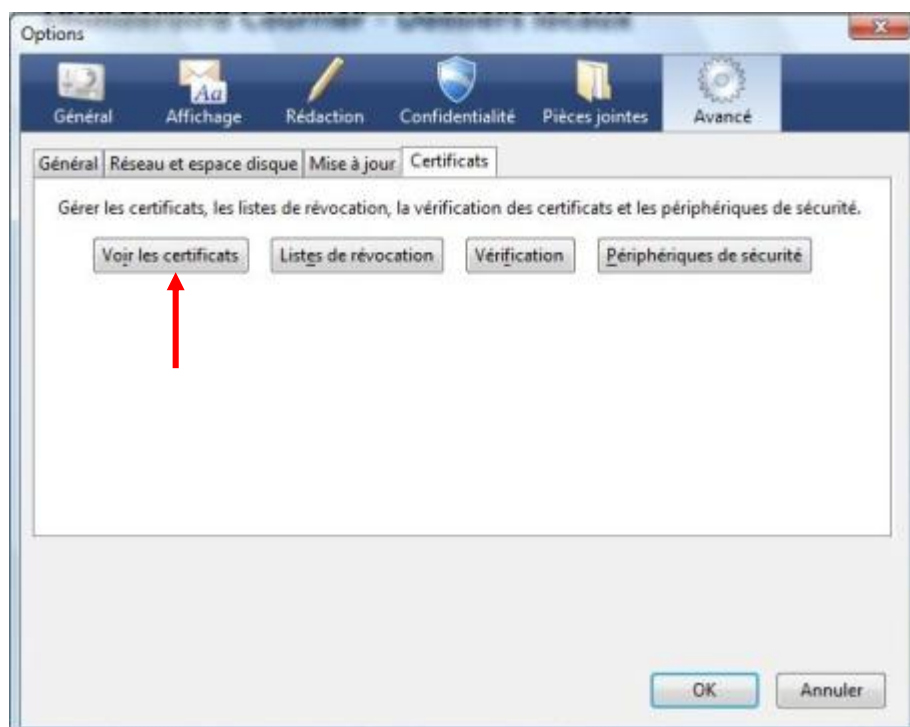
Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



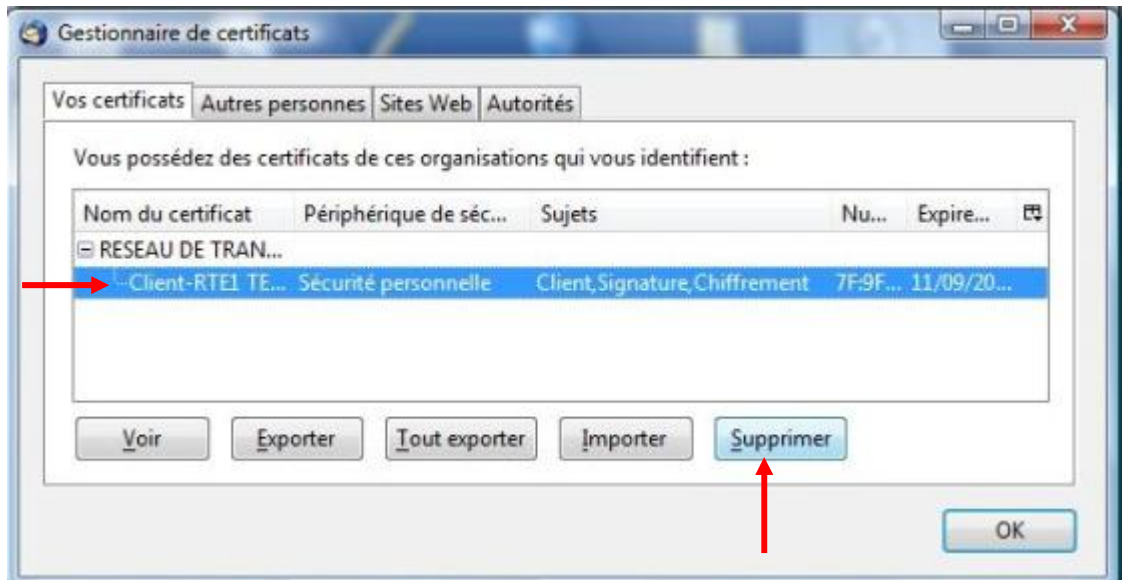
13.4 Deletion of the certificate

With Mozilla Thunderbird (v. 1.5), deletion of a certificate with the private key.

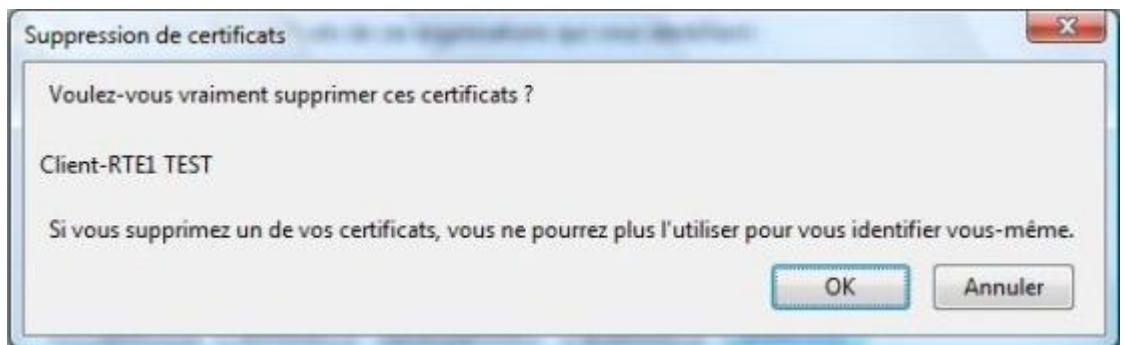
Open the "Tools > Options..." menu, the "Confidentiality" section and then the "Advanced" tab (v. 1.5 and higher):



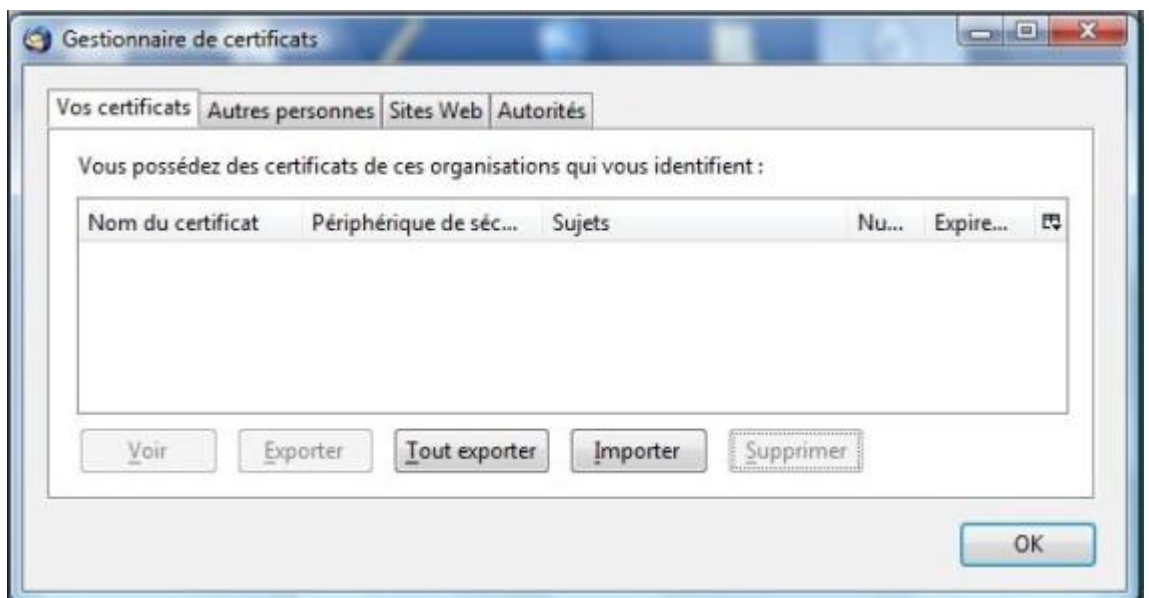
Click on the "View the certificates" button.



Select the certificate to be deleted and click on "Delete"



Confirm the validation by clicking on the "OK" button.



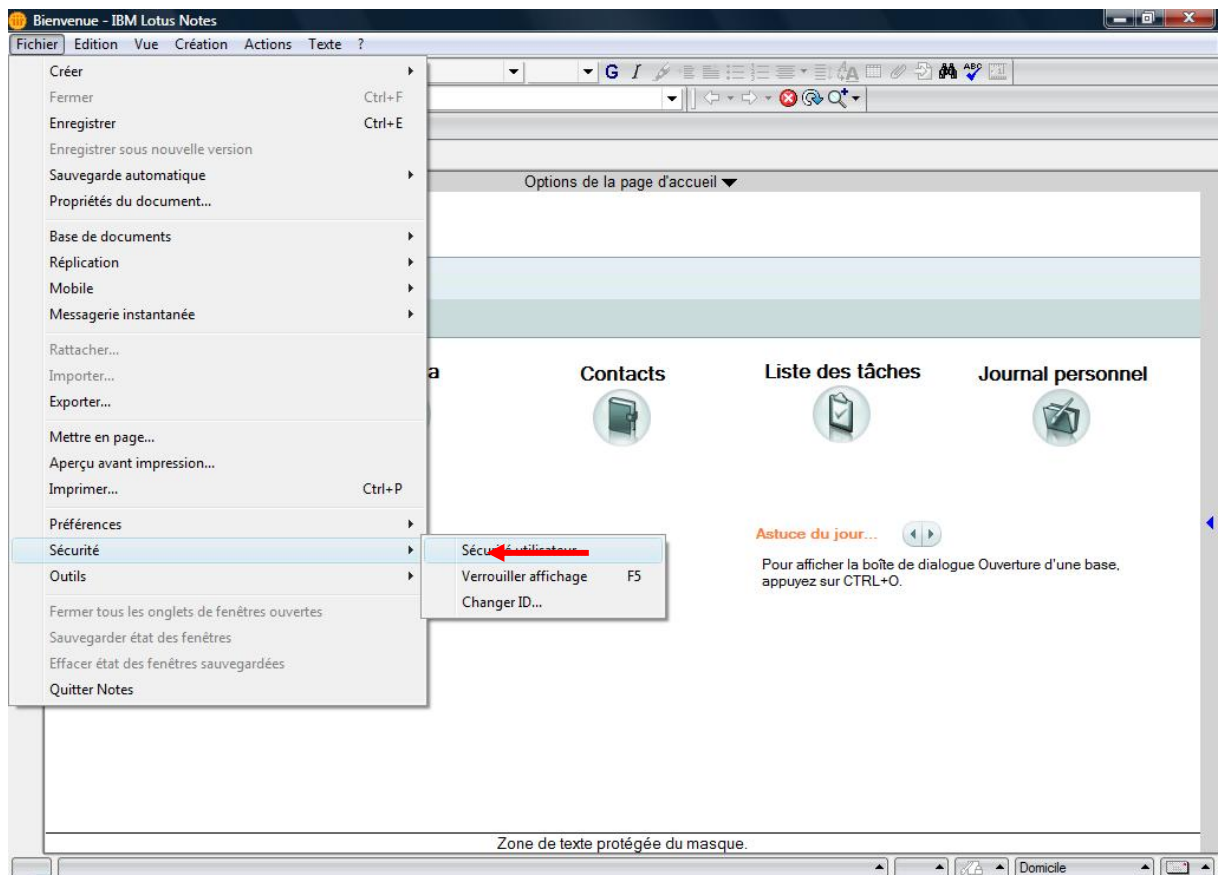
The certificate is deleted from the certificate list.

14. Lotus Notes



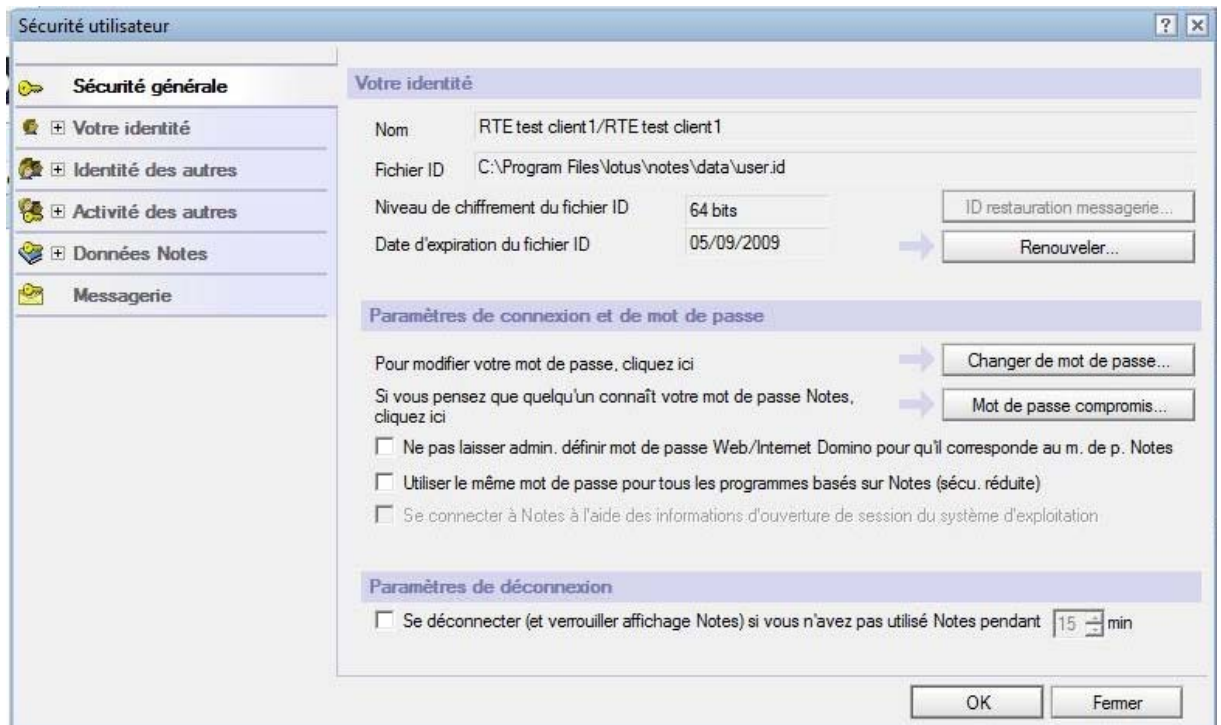
14.1 Importing the certificate

Start Lotus Notes R7 and use the "File > Security > User security..." menu option:

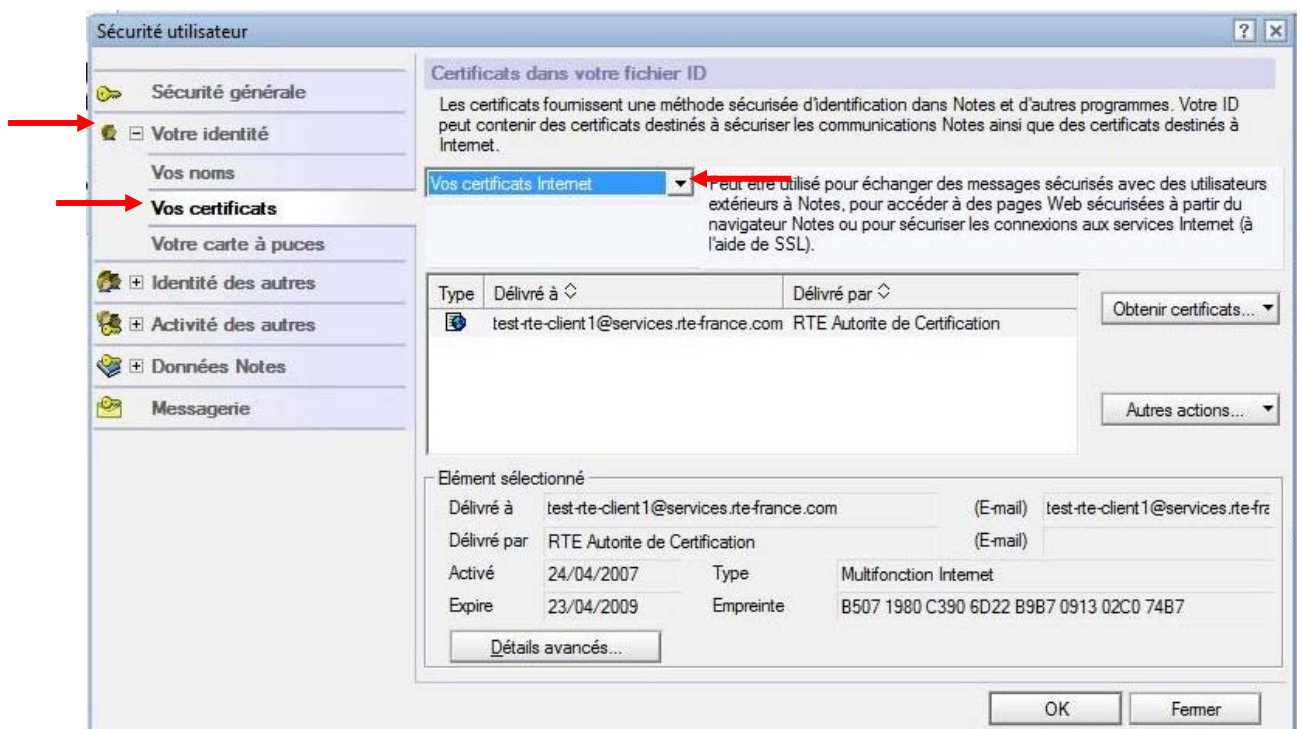


The following screen is displayed:

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



Click on "Your identity" and then on "Your certificates":

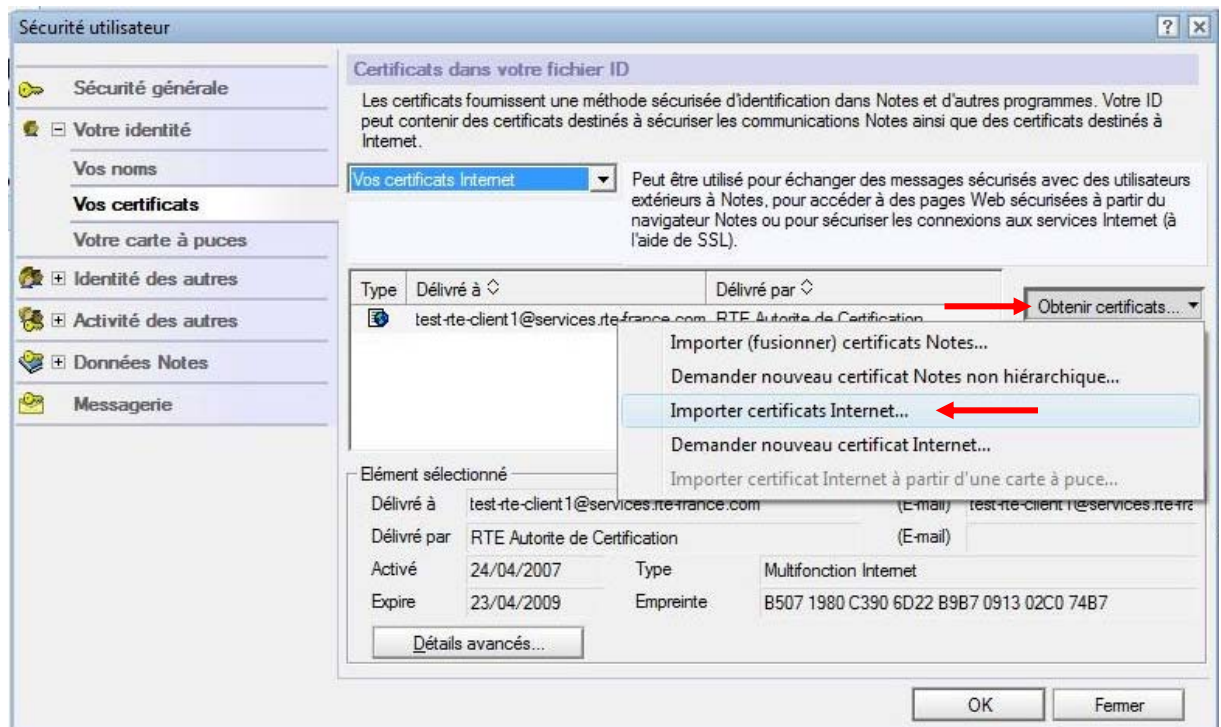


Now select "Your Internet certificates" from the dropdown list so that any Internet certificates already imported are displayed.

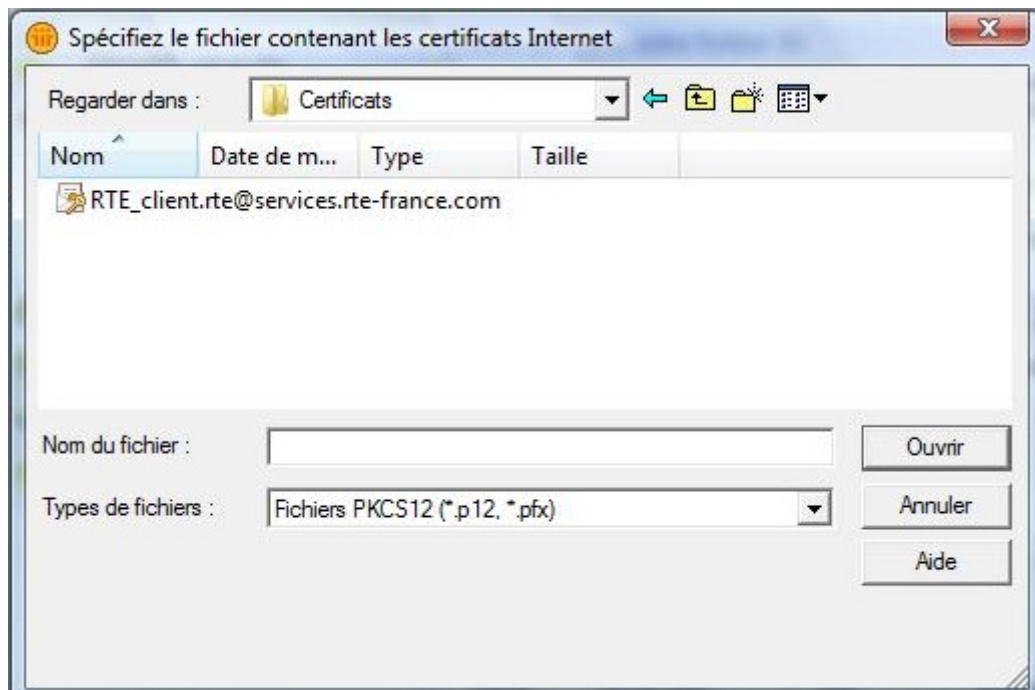
Generally speaking, the list will be empty.

Click on the "Obtain certificates" button and select "Import Internet certificates":

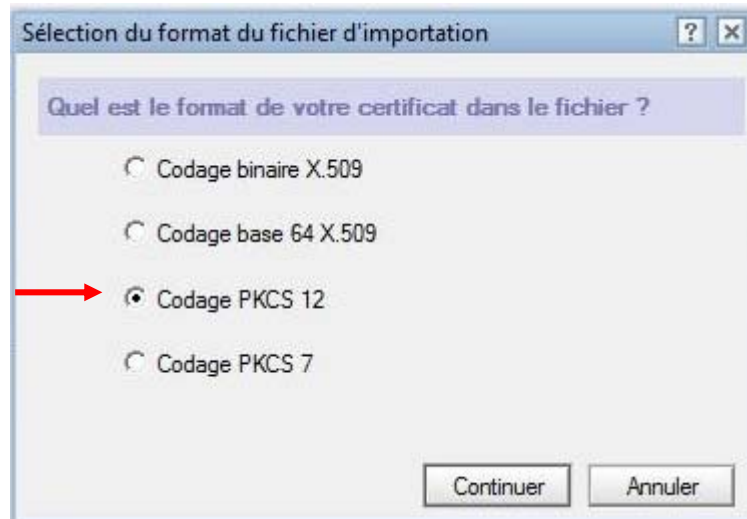
Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



A search window will be displayed: select the PKCS#12 file (with either a .p12 or .pfx extension) that contains the certificate to be imported, as well as its private key and the RTE CA root key:



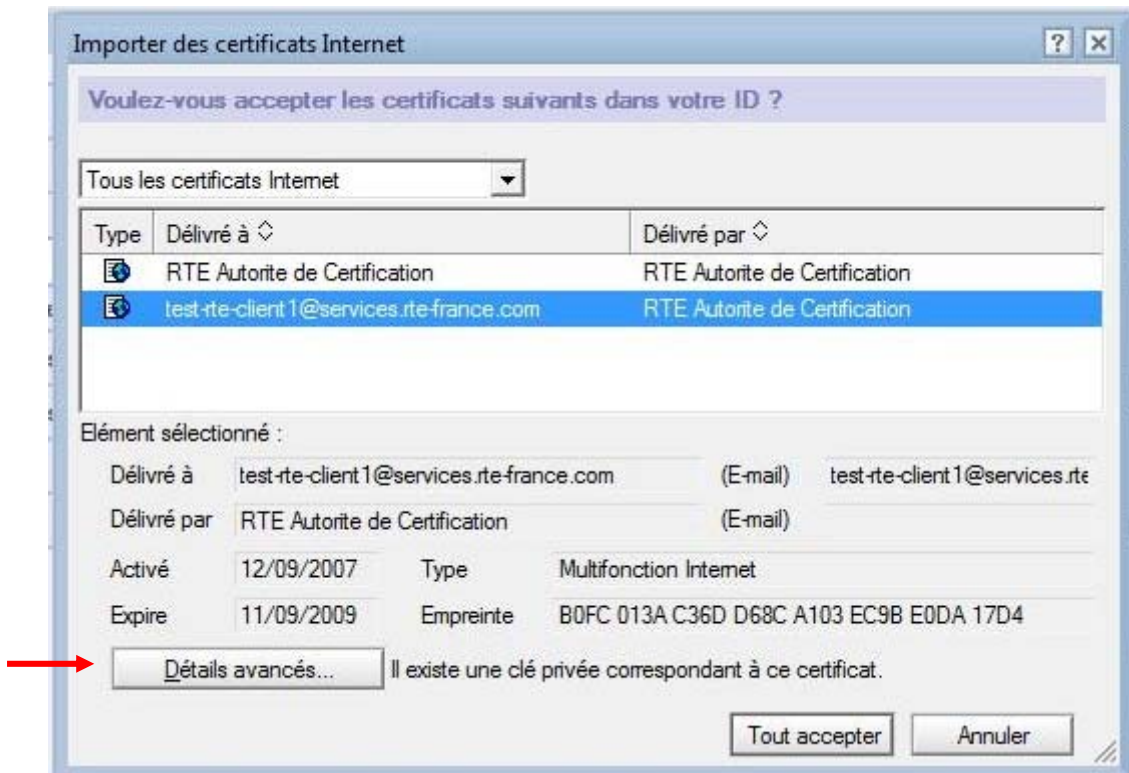
Click on "Open" and in the window below, select the PKCS12 encoding:



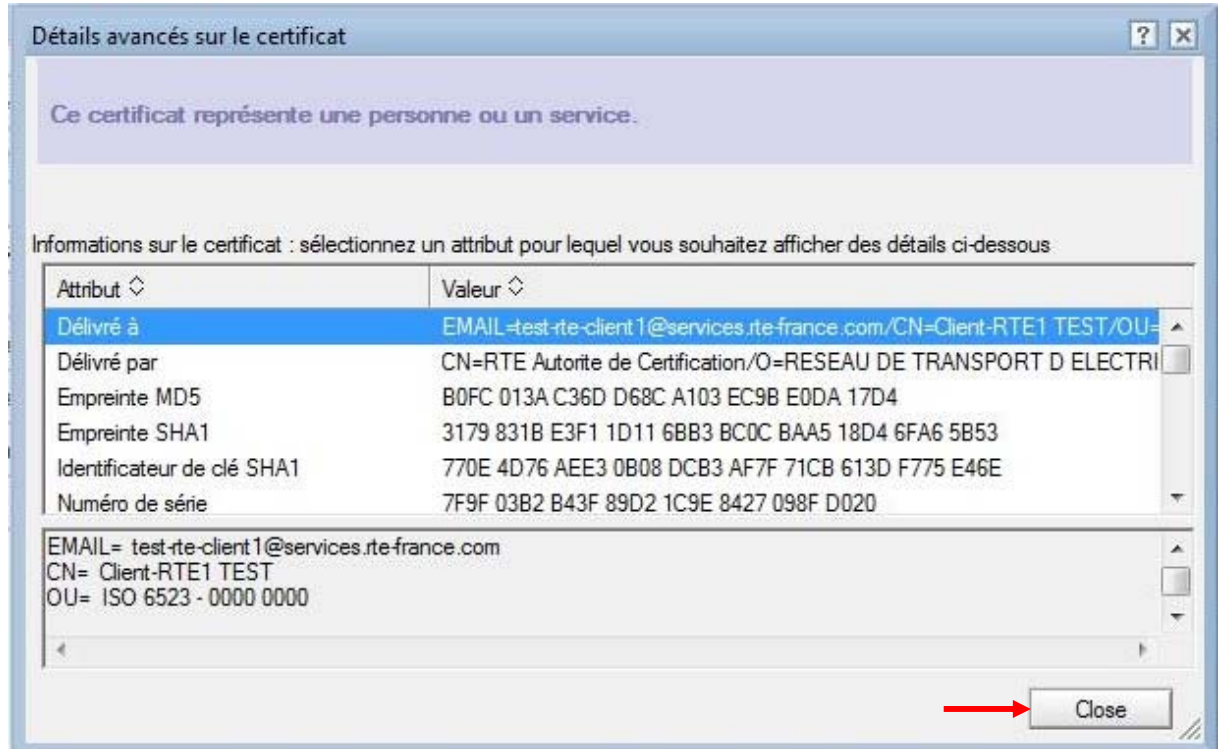
Click on "Continue". The PKCS12 file protection password will then be requested:



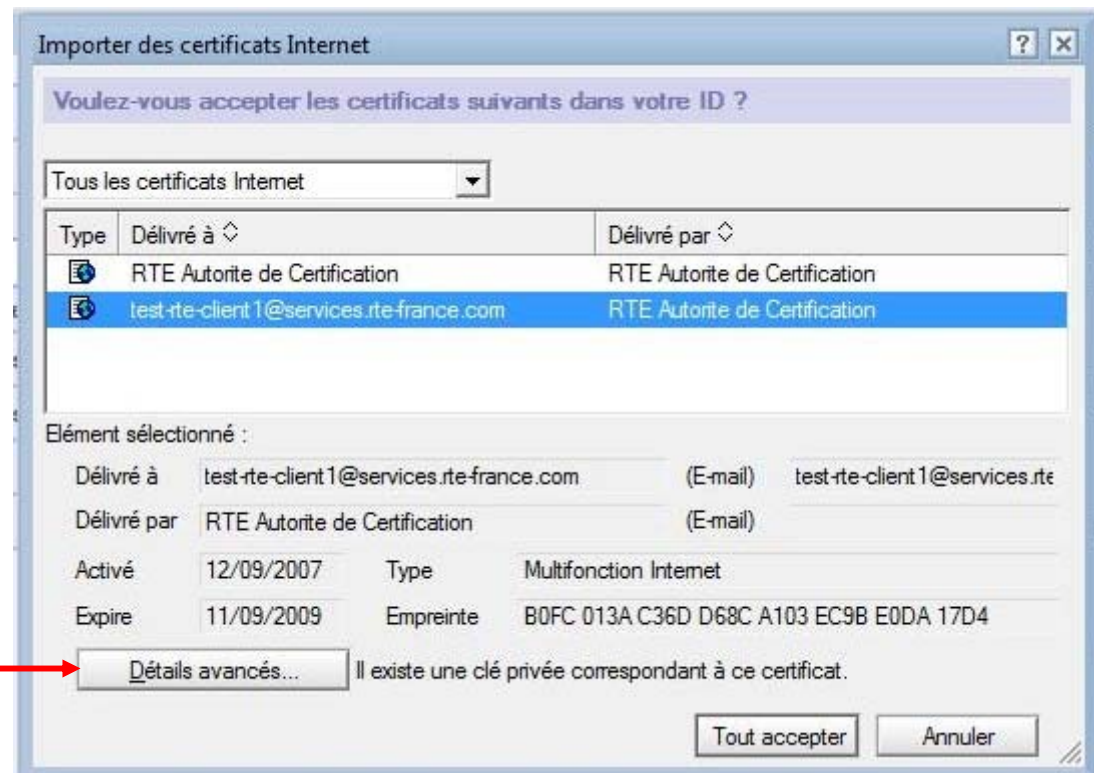
Click on "OK" and the following window is displayed:



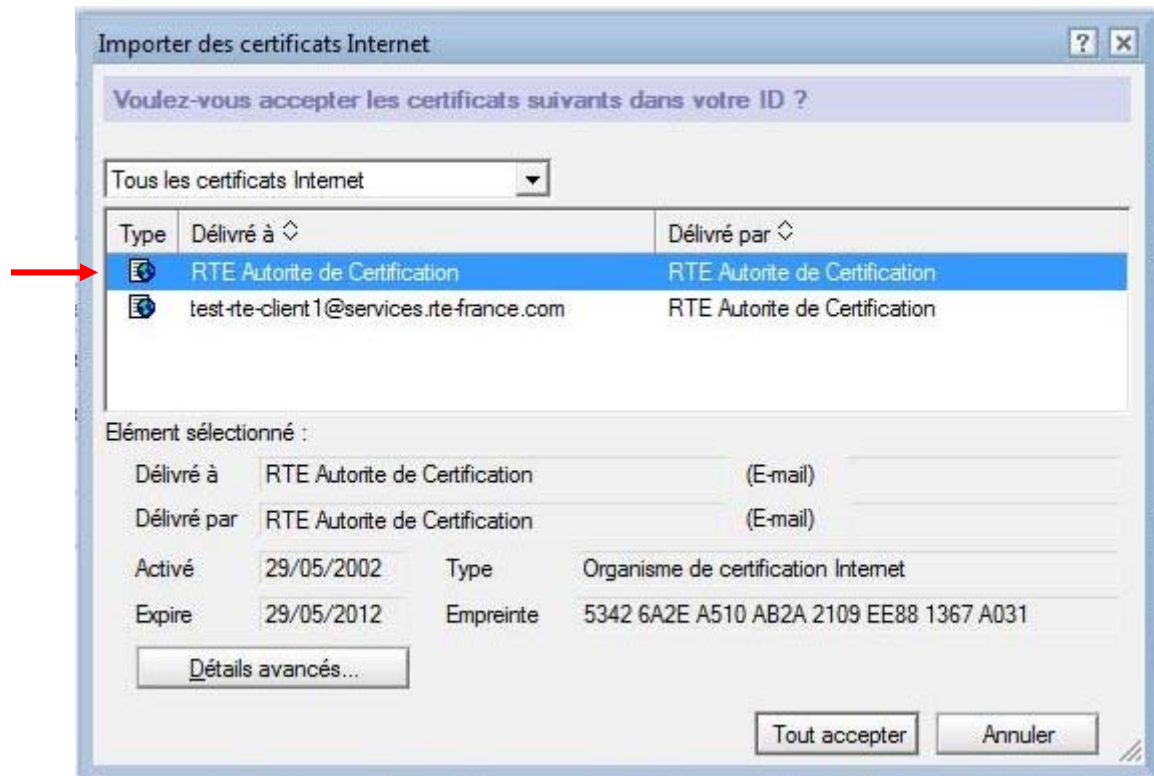
Your certificate that you wish to import, as well as the root certificate, are shown in the list. If you click on "Advanced details", the contents of the selected certificate (your certificate, in this example) are displayed in the following window:



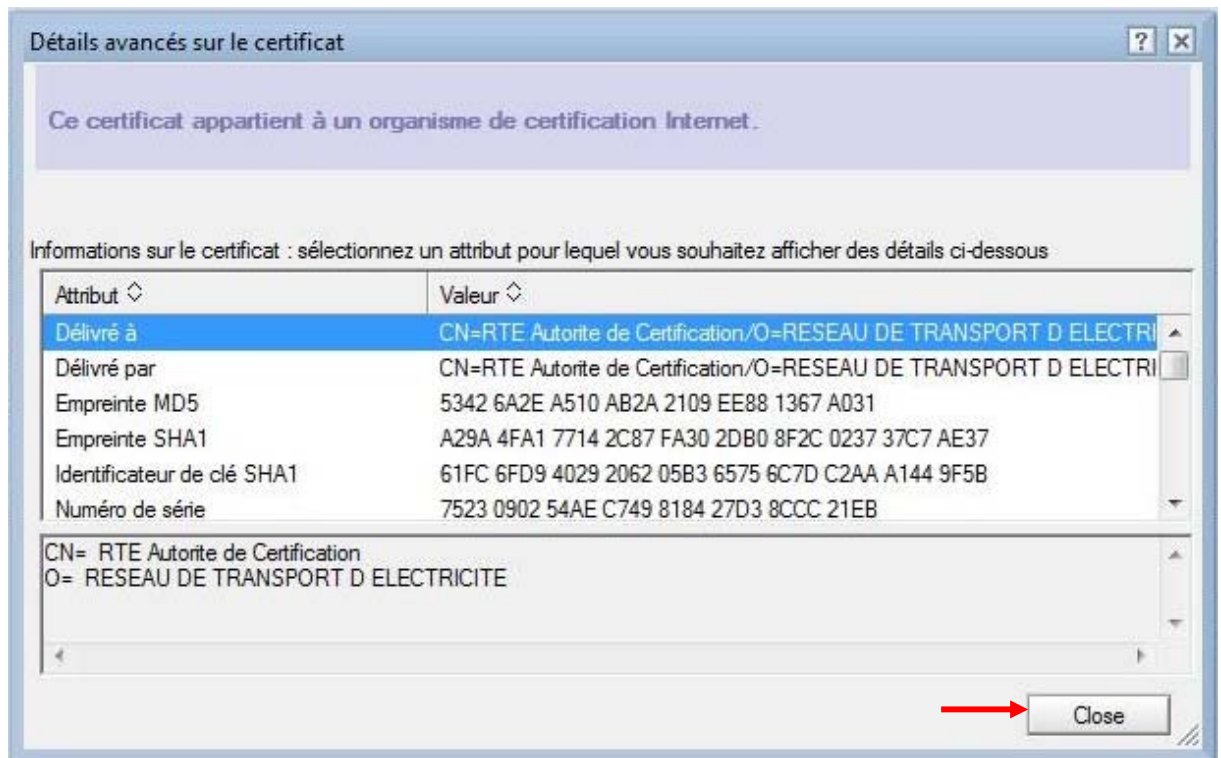
Click on "Close" to return to the preceding window:



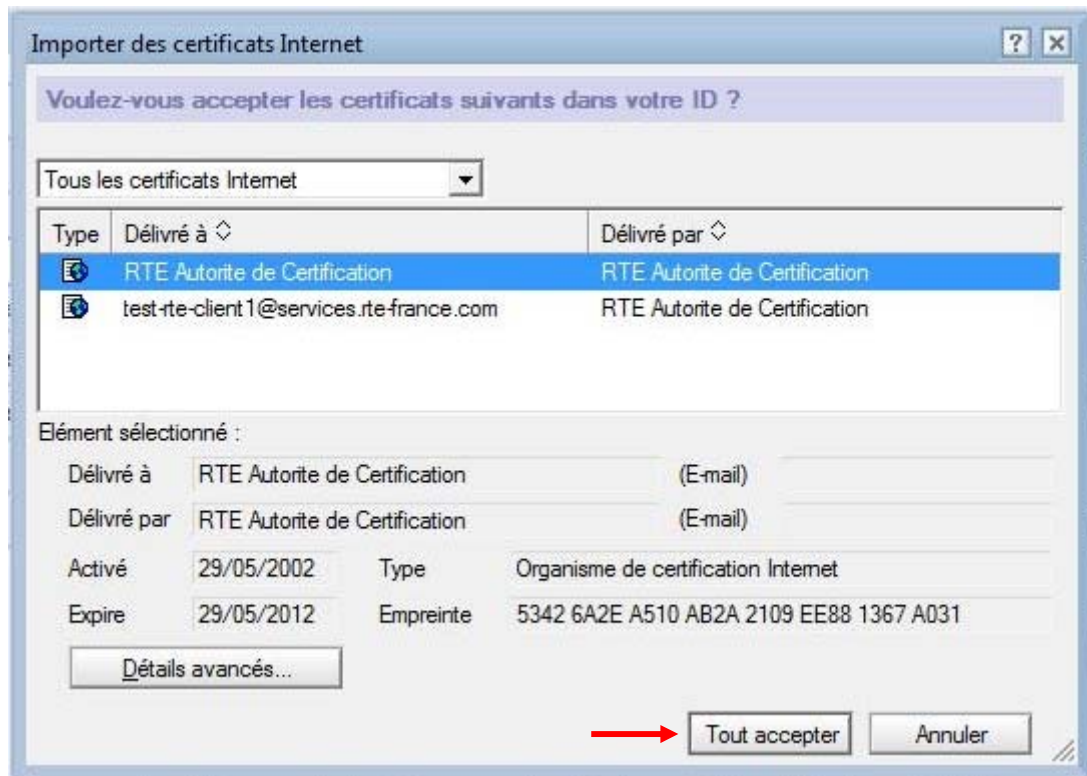
To see the contents of the root certificate, you must first select it:



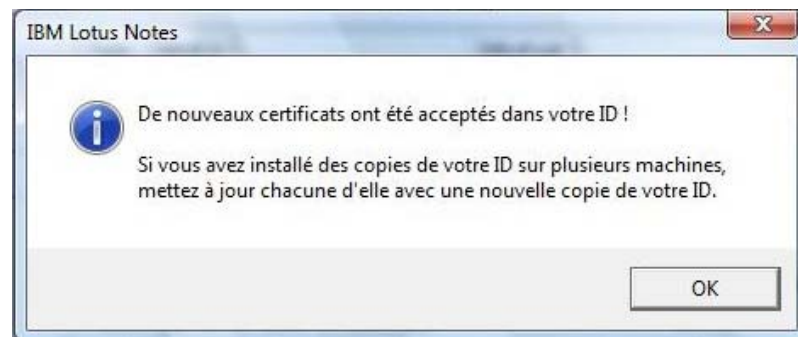
before clicking on "Advanced details":



Click on "Close" to return to the original screen:

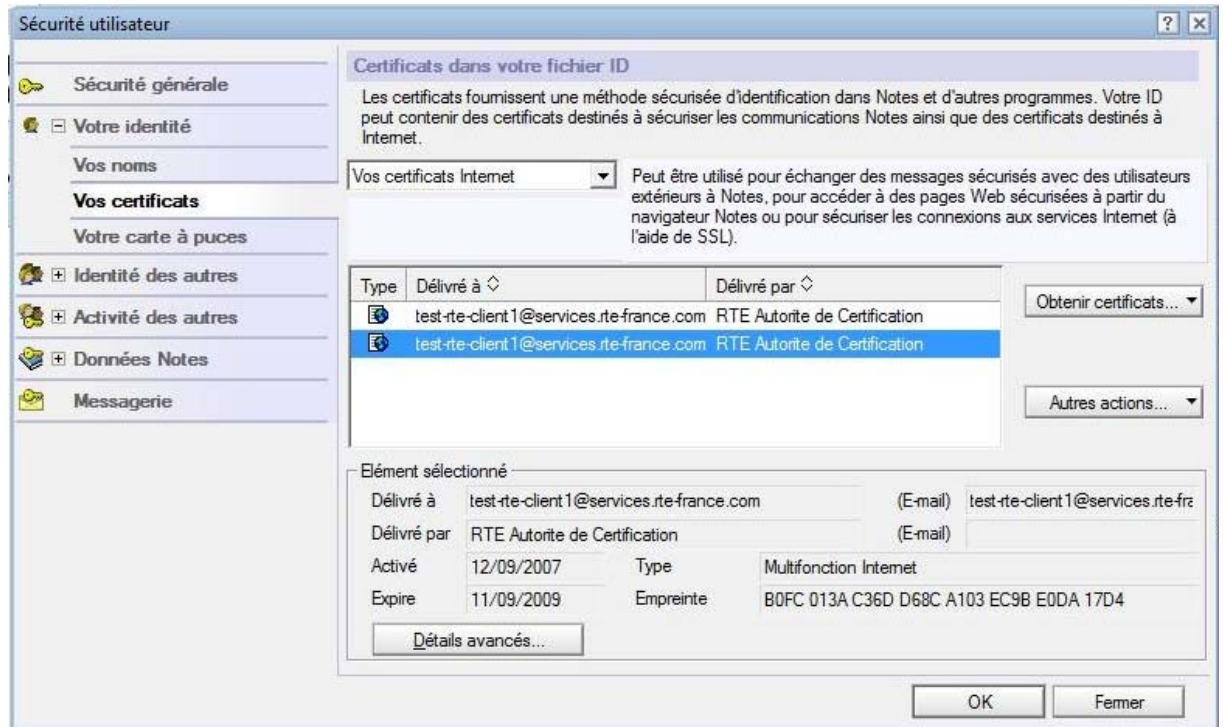


Click on "Accept all":



Click on "OK" and the following window is displayed:

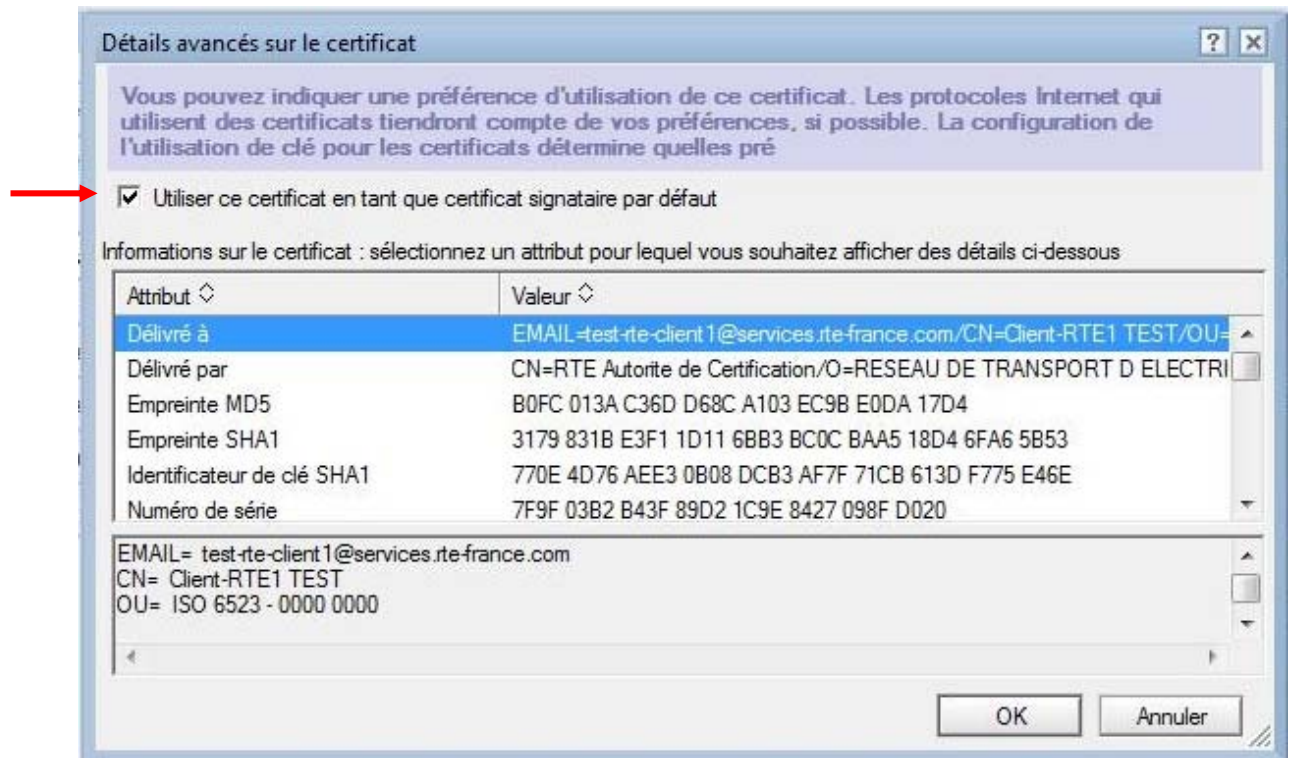
Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



The certificate, now visible in this case, has indeed been imported. Click on "OK" to finish this import.

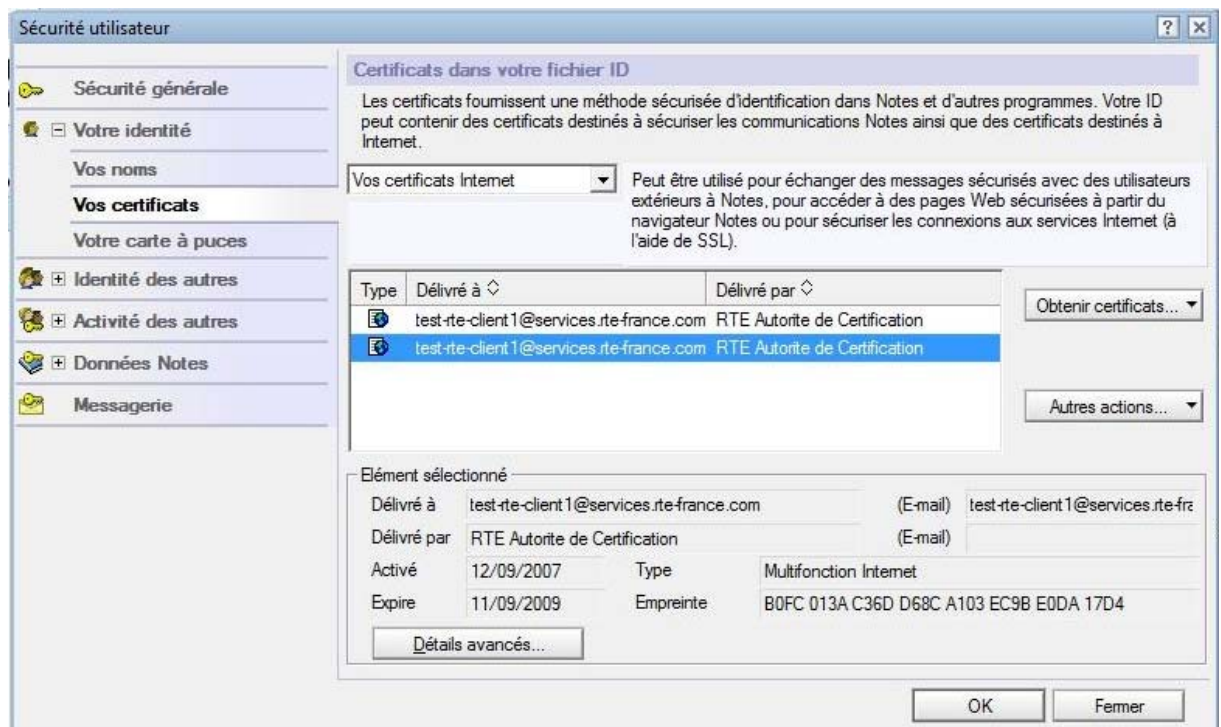
NB:

If you have several certificates usable for signing your outbound messages, you must select as a default the one which you will use for communications with RTE. Before clicking on "OK" in the screen above, select your certificate and click on the "Advanced details" button so that you can check the "Use this certificate as the default signing certificate" checkbox, just as shown in the screen image below:



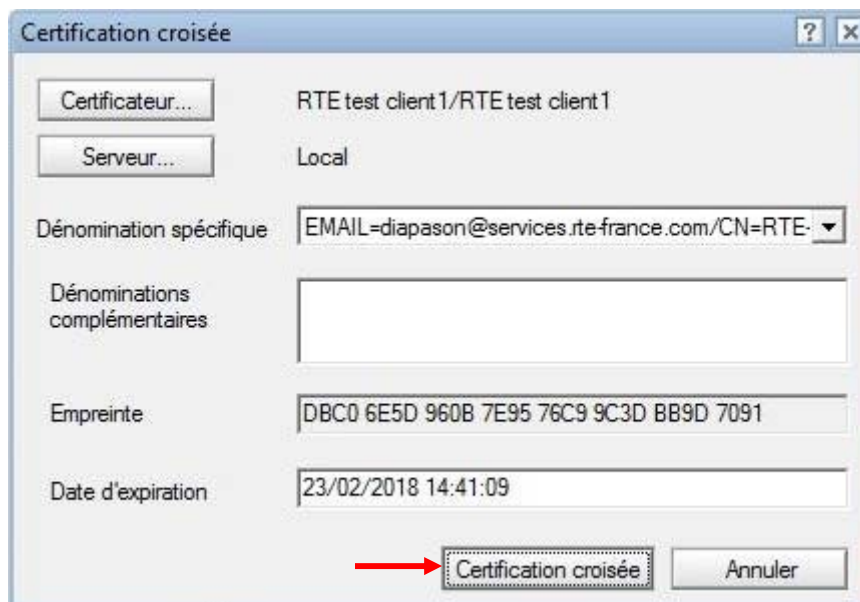
14.2 Viewing the certificate

To view your certificate, you only need to select the certificate and click on "Advanced details" in the following window, that, as before, can be opened through "File > Security > User security":



14.3 Reception of a signed and encrypted message

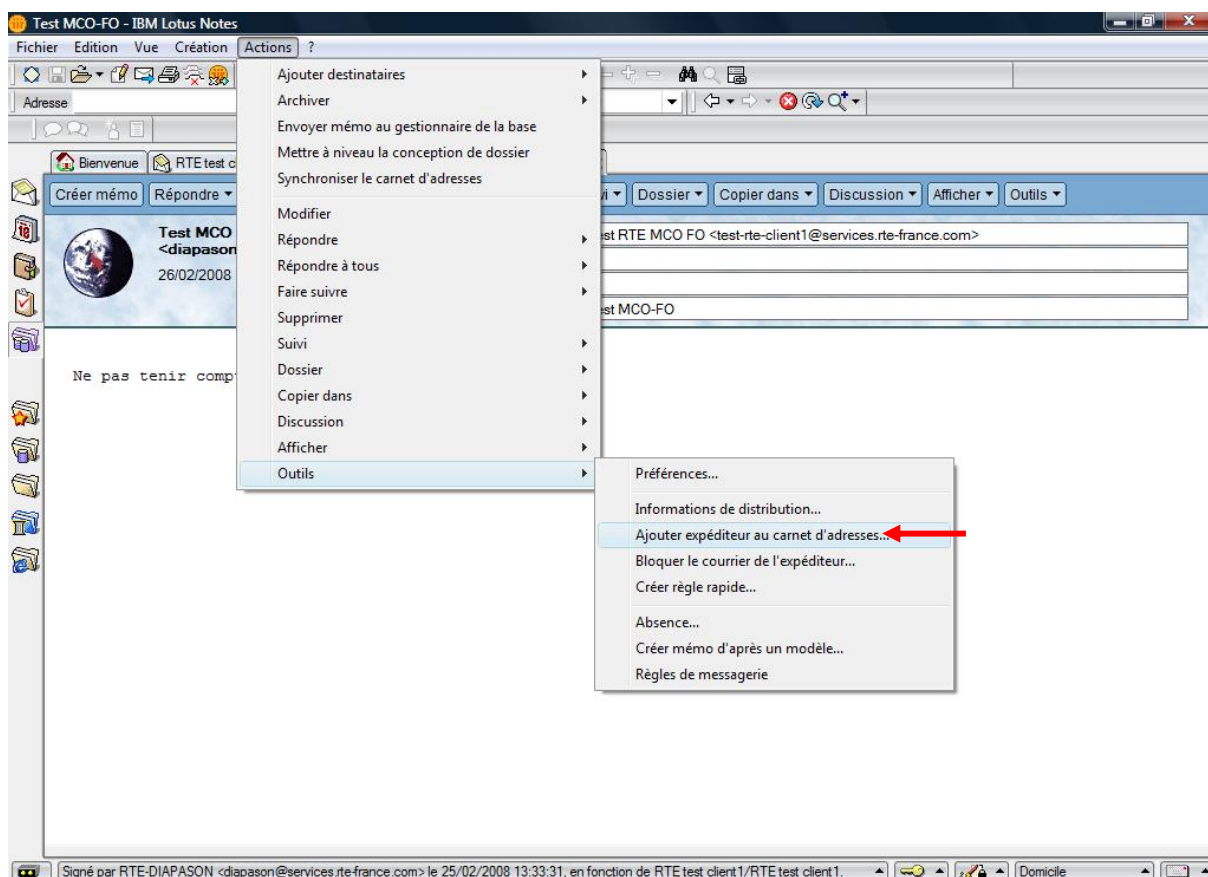
The first time that you select a signed message that you have received, a dialogue box similar to the one below will be displayed, so that you can grant your confidence in the sender:



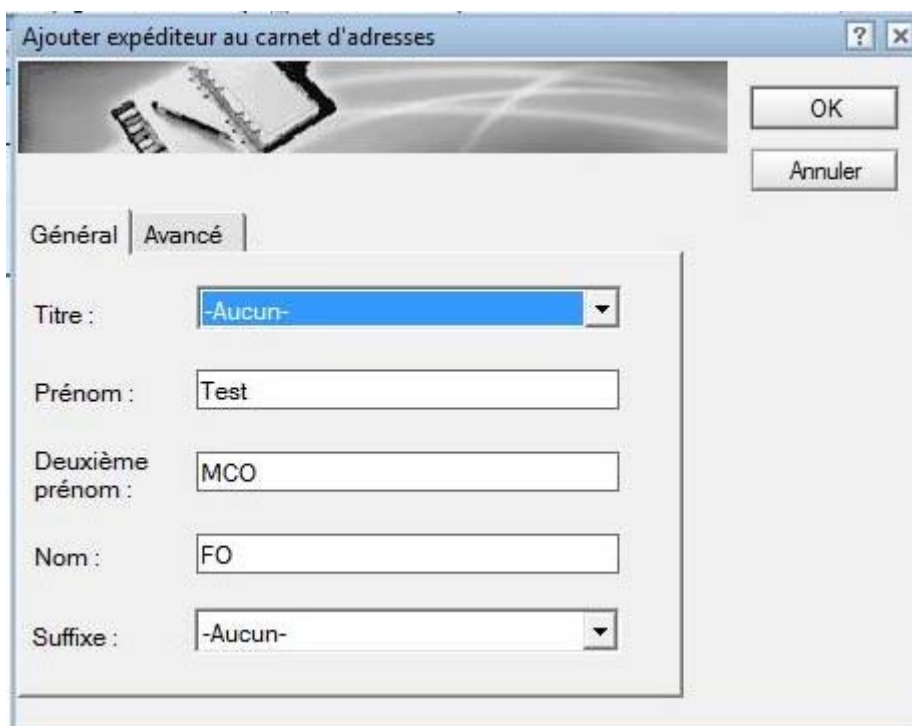
To do so, you must click on the "Reciprocal certification" button.

Then, while you are reading the signed message that you received, you should select the "Add sender to the address book" function, which will add your contact and his certificate into your address book:

Access to the IT system with digital certificates under Microsoft Windows Vista PKI user manual



The following window will then be displayed:

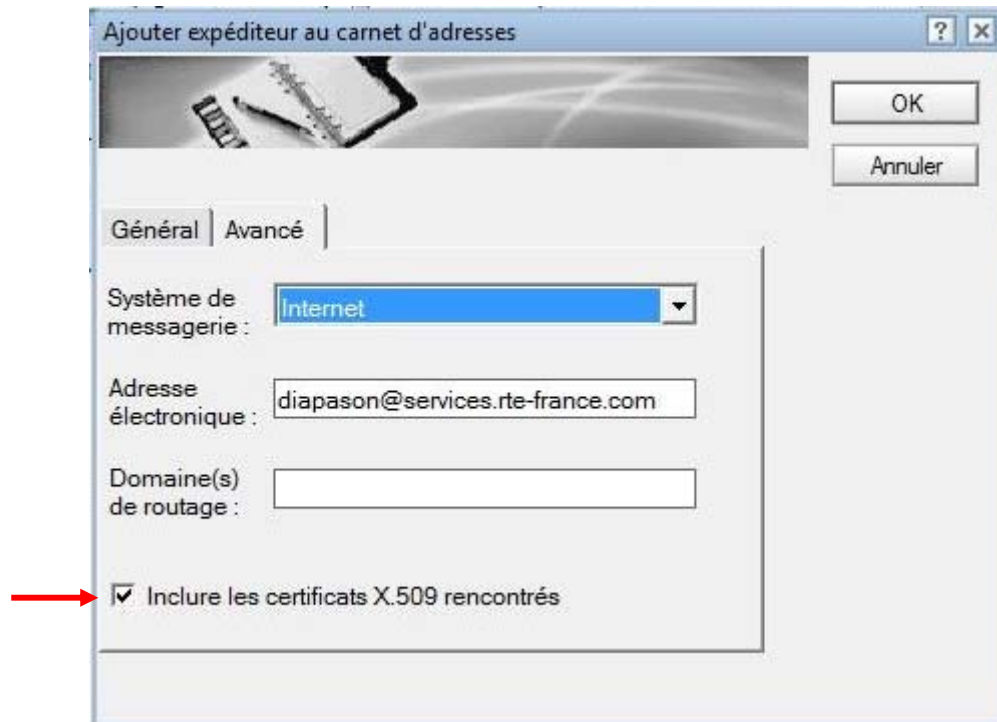


The screenshot shows the 'Ajouter expéditeur au carnet d'adresses' (Add sender to address book) dialog box. The dialog has two tabs: 'Général' (General) and 'Avancé' (Advanced). The 'Général' tab is currently selected. It contains the following fields:

- Titre :** A dropdown menu with '-Aucun-' (None) selected.
- Prénom :** A text field containing 'Test'.
- Deuxième prénom :** A text field containing 'MCO'.
- Nom :** A text field containing 'FO'.
- Suffixe :** A dropdown menu with '-Aucun-' (None) selected.

At the bottom right of the dialog, there are two buttons: 'OK' and 'Annuler' (Cancel).

Open the "Advanced" tab:



Just confirm that the "Include X.509 certificates found" checkbox is checked, and click on "OK".

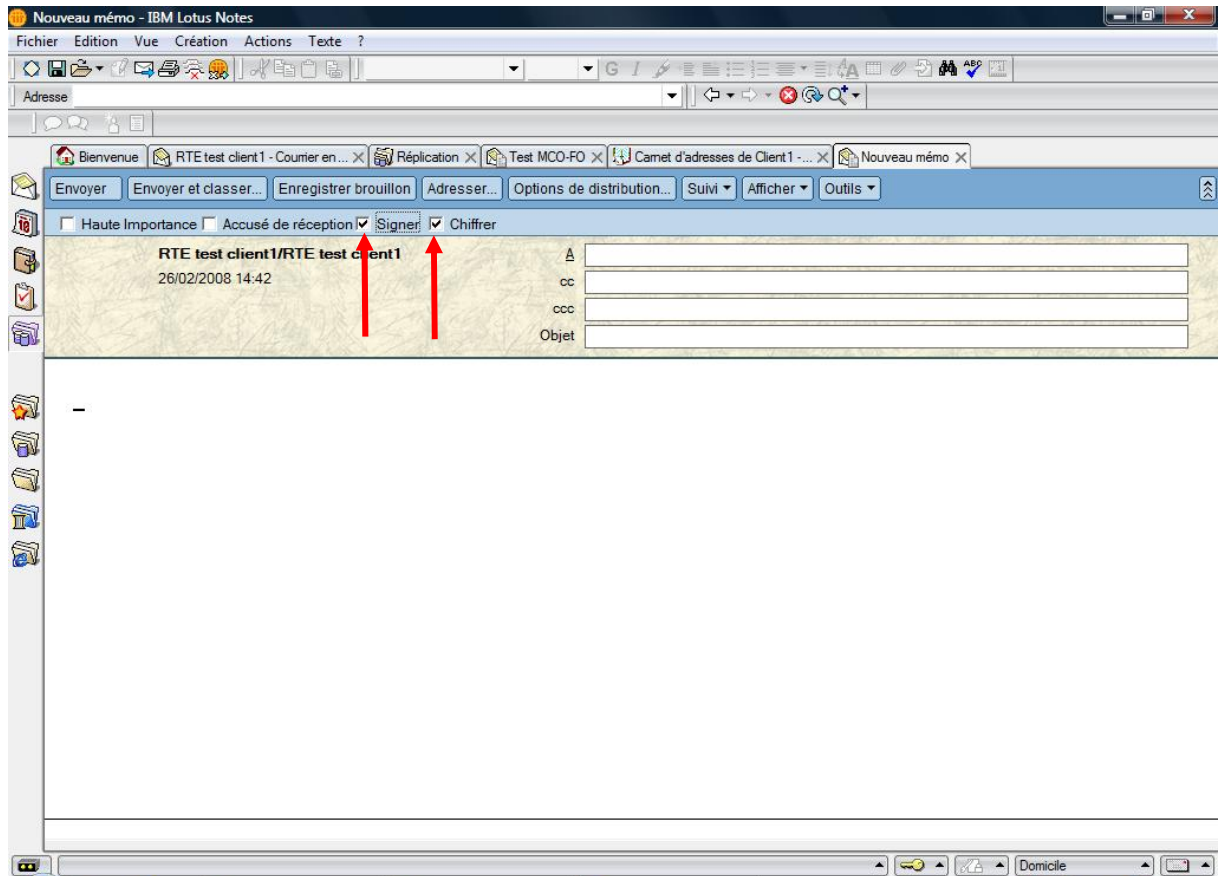
From here on, you can encrypt any message sent to this contact.

14.4 Signature and encryption of messages sent

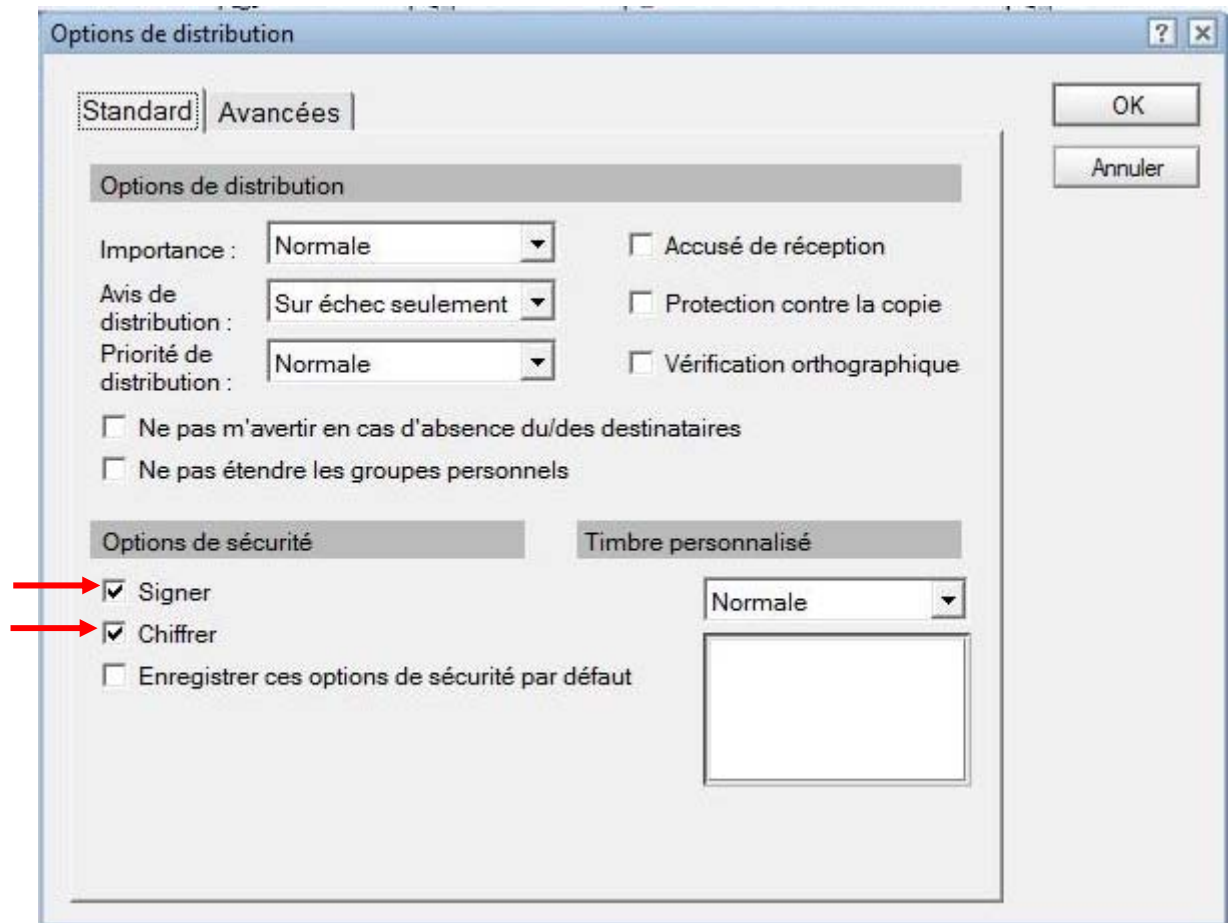
When you compose a message, you can sign and encrypt it if you have your own signature certificate (refer to the 'Importing the certificate' section above) and that of your correspondent.

To do this, whenever you create a new memo, you should check the "Sign" and "Encrypt" boxes as illustrated below:

Access to the IT system with digital certificates
under Microsoft Windows Vista
PKI user manual



You may alternatively click on the "Distribution options" button and check the "Sign" and "Encrypt" boxes as shown below:



The rest of the message sending procedure is exactly the same as normal, with Notes taking care of signing and encrypting the message transparently.



F. APPENDICES

15. PKI Secured environments

This appendix describes the secured environment in which the PKI system is implemented. It specifically addresses:

- the concepts of the secured environment and the corresponding computing objects managed by the PKI,
- the role of the different entities taking part in the PKI operational processes.

15.1 Concepts and objects generated by a PKI

This appendix presents the principal concepts needed to understand the role of the objects generated by a PKI:

- a presentation of the structural principles of a secured process,
- the role of the key pair,
- and the certificates.

15.1.1 What is a secured process?

15.1.1.1 Definition of a PKI

With a PKI (Public Key Infrastructure, or IGC in French for Infrastructure de Gestion de Clés), every certificate holder has a pair of keys – a private key, known only to its sole owner, and a public key – inter-connected with a complex mathematical relationship, which makes it almost impossible to determine the private key with only the public key. This means that the probability of determining the private key based on the public key in a **reasonable** period of time is **very low**.

Data encrypted with one key (typically the public key) can only be decrypted using the other one (typically the private key). This is the basis which forms the core operation that ensures the confidentiality of the exchanged messages.

15.1.1.2 The four pillars of information communication security

This electronic identity card is designed to establish a trust environment based on the four following fundamental pillars:

- **authentication** confirms that the participant parties are indeed who they claim to be;
- **confidentiality** prevents non-recipients from reading the data;
- **integrity** ensures that the data have not been altered in transit;
- **non-repudiation** makes it impossible for either party to deny that the information has been transmitted.

15.1.1.3 The cryptographic solution

Because of the inherent nature of the technology used (i.e. public protocols, architectures, etc.), information circulating on the Internet is not

confidential. Neither do the technologies currently employed respond to the other three security requirements mentioned above.

In order to maintain the confidentiality of communications made over the Internet, the data must be rendered incomprehensible to anyone except the intended recipients. Encryption is a solution that meets these demands.

The encryption of the data is naturally accompanied by the authentication of the system users. In reality, if certain data are confidential, it is necessary that the senders and receivers of that data can authenticate each other in a certain and unambiguous manner in order to proceed with secured communications.

Authentication relies on the possession of a certificate. This certificate is delivered by a Certification Authority to which the participating parties of a transaction both assign confidence (in our case, the Certification Authority is the RTE). In addition, certificate holders can trust the information supplied to them, and RTE knows that only the assigned certificate holders have access to the information.

NOTE

Following an analogy in normal life, it is necessary to supply an identity document provided by an approved authority in order to have access to certain privileges reserved for citizens of a country (e.g. very expensive purchases, exercising voting rights, etc.).

15.1.2 The role of the key pair

Each certificate holder has a public key as well as a corresponding private key:

- The **private key** is the key that the certificate holder must keep confidential. He is the only person to **have that key and be able to use it**. He may not necessarily know it himself (for example, it might be stored on a card with a computer chip, from which it can be extracted, but access to the card is protected with a PIN code known only by its owner).
- The **public key**, as its name indicates, is public and may be communicated to everyone. The public keys of certificate holders are only used to encrypt messages intended for the certificate's holder. If an encrypted message is intercepted, there are no significant impacts to confidentiality because the message can not be decrypted (in a reasonable period of time) by a person who does not have the private key.

The private key enables its owner to sign messages that he sends out and to decrypt messages that are sent to him.

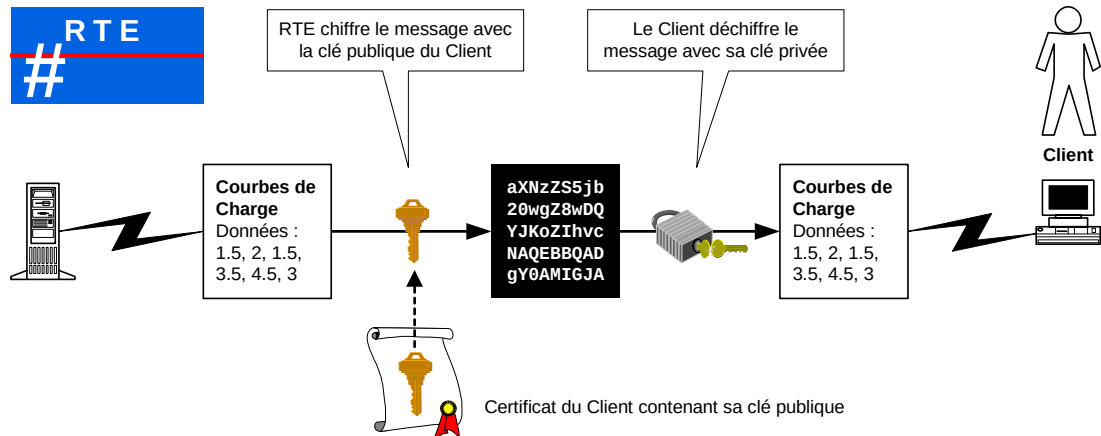
15.1.2.1 Encryption and decryption of a message

Each message is encrypted with the public key of its recipient, who will decrypt that message with his private key.

When RTE sends a message to its customer A:

1. RTE knows the public key of customer A (from his certificate).

2. RTE automatically encrypts the message using customer A's public key and sends it to him using RTE's electronic email services.
3. Customer A receives the message and automatically decrypts it with his private key.

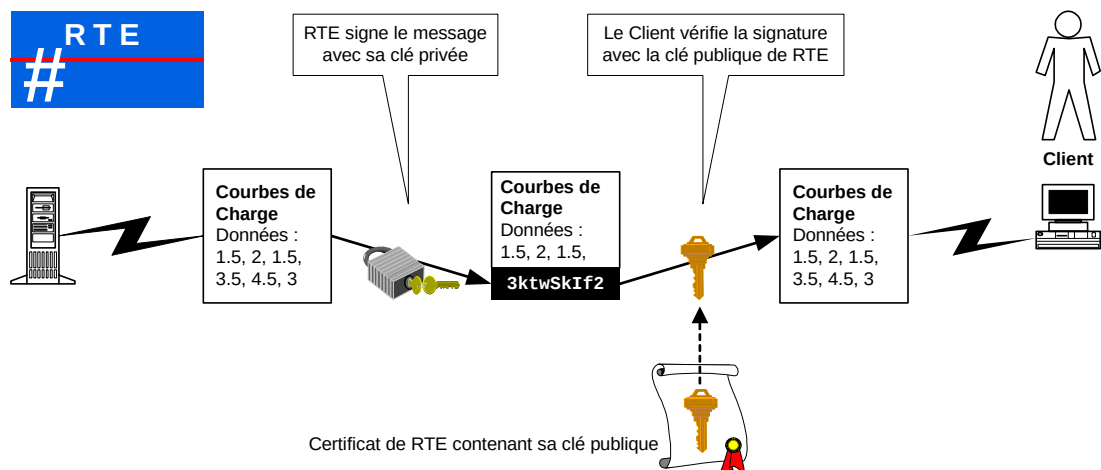


Encryption and decryption with a key pair

15.1.2.2 Use of the keys for signing messages

Each message is signed with the private key of the sender. The source (i.e. the signature) of a message can be checked thanks to the sender's public key being openly available through his certificate.

To prove to customer A that the message he has received actually does come from RTE, RTE automatically signs its messages with its own private key before sending them to customer A.



Signing and signature verification with a key pair

When customer A receives the message from RTE, he automatically verifies the signature on the received message with RTE's public key.

15.1.3 The certificates

15.1.3.1 Objectives of the digital certificate

Because the public keys are used to verify the electronic signatures and to encrypt messages, it is critical for every certificate holder to be certain about the identity of the owner of a public key: this is the role of the **certificate**.

15.1.3.2 Properties of a certificate

The certificate is an electronic proof of identity:

- which guarantees the identity of its holder,
- which contains data facilitating identification,
- which is resistant to counterfeits and is issued by a trusted third party: the Certification Authority.

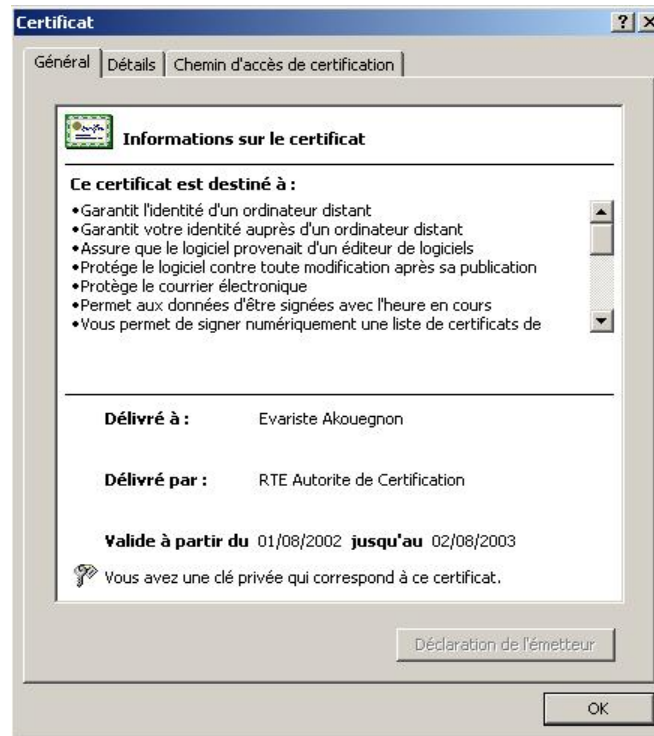
A Certification Authority is an entity which creates and manages certificates. It defines the rules for registration in the PKI of the various certificate holders.

15.1.3.3 Structure of a certificate

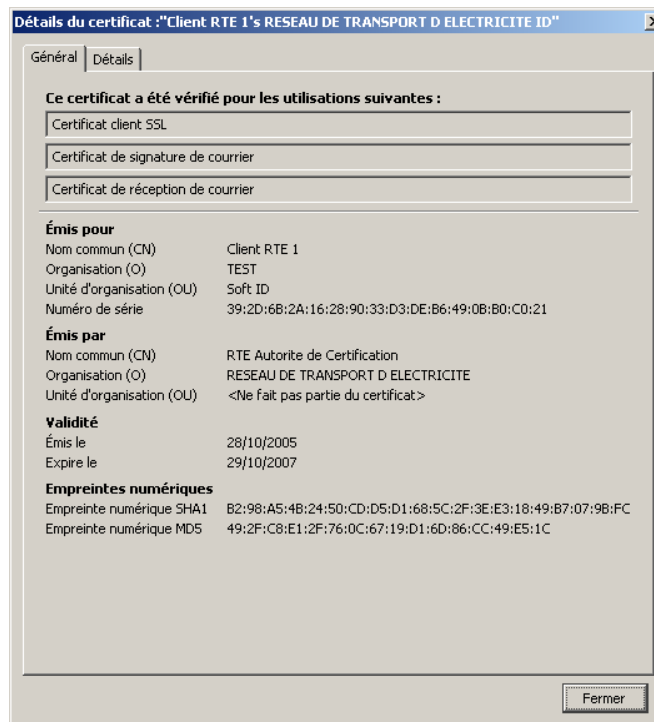
A digital certificate contains:

- the **public key** of the owner,
- the **name of the owner** and other identification information (the email address of the person if it is a certificate to be used to sign emails),
- the **validity period** of the certificate,
- the **name of the certification authority** which generated this certificate,
- a unique **serial number**,
- and the **signature** of the certification authority.

15.1.3.4 Certificate examples



A digital certificate in Internet Explorer



A digital certificate in Mozilla Firefox

15.2 Documentation

Reference documents:



- The RTE Certification Policy,
- The subscription contract for the RTE's secured IT system.

Web sites:

- **<http://www.legifrance.gouv.fr/>**
- Legislation from March 13th 2000 bearing modifications on legal proofs of information technologies relative to electronic signatures:
<http://www.assemblee-nat.fr/>
- Directive 1999/93/CE from December 13th 1999 concerning an EU community framework for electronic signatures:
<http://europa.eu.int/>
- The regulatory working group on electronic signatures:
<http://www.internet.gouv.fr/>
- Keynectis:
<http://www.keynectis.com/>

16. Glossary

When certificate holders approach their new secure environment, they will be confronted with specific terminology, the terms of which are explained in this section.

- **Authentication**

Verification of the validity of identity as declared by a user, by a device or by another entity in an information or communications system.

- **Certification Authority**

A Certification Authority (CA) is an entity which issues digital certificates for use by other parties as electronic equivalents of identity documents. In distributing digital certificates, the Certification Authority or Trust Authority serves as an ethical guarantor by asserting a person's identity through the certificate provided to that person. According to the scope accorded to the Certification Authority, this certificate will have a field of application of varying range: limited to internal communications in a company (like a company security badge) or for use in communications with other organisations and administrative bodies (like a national identity card or passport).

- **Certificate**

A digital certificate plays the role of an electronic ID card (electronic passport). It guarantees the identity of its owner in electronic transactions and contains all the information required to permit such identification (surname, first name, possibly company, address, etc.). A digital certificate consists of a public key and personal information about the holder, all signed by a Certification Authority.

- **Confidentiality**

A property of data or information which are neither actively nor passively available nor disclosed to unauthorised persons.

- **Cryptography**

The practice, study and techniques of transforming data with the aim of hiding its semantic content, establishing its authenticity, preventing its unobserved modification, warning of its repudiation, and preventing its unauthorised use.

- **Private Key**

A secret digital value assigned to one person, allowing that person to either successfully decipher messages encrypted with the corresponding public key or to affix an authenticating signature to the foot of messages sent.

- **Public key**

A digital value, assigned to one person, but distributed to others so that these others are able to either securely send the person encrypted data or to verify that person's signature.

- **Encryption / Decryption**

The transformation of data through cryptographic techniques to make that data unintelligible in order to ensure its confidentiality / The inverse transformation of encrypted data.

- **Integrity**

The assurance that the data or information have not been modified or altered in an unauthorised manner.

- **Non-repudiation**

A property obtained with cryptographic methods to prevent a person from denying having performed a particular action on the data (for example, source non-repudiation; attestation of obligations, intentions or commitments; establishment of ownership).

- **Revocation**

Revocation is the procedure which leads to the deletion of the guarantee provided by the Certification Authority for a given certificate, made upon the request of the subscriber or any other suitably authorised person. The request may be the consequence of various types of events, such as the compromise or destruction of the private key, the modification of information contained in the certificate, or non-respect of the certificate's usage rules.

- **Electronic signature**

The electronic signature of a document consists of signing a digital "summary" of that document with one's private key, which can then not be modified without such modification being visible. As with a handwritten signature, it commits the signatory to certain responsibilities.

- **Virtual private network (VPN)**

A Virtual Private Network makes it possible to make connections between disparate local networks using a tunnelling technique. The tunnel is a secured Internet communications channel through which data is transmitted with embedded encryption.

END OF DOCUMENT